COUNTERBOMB

PROTECTING YOURSELF AGAINST CAR, MAIL, AND AREA-EMPLACED BOMBS

LAWRENCE W. MYERS

From 1983 to 1988, the use of IEDs (improvised explosive devices) as murder weapons in the United States increased more than 430 percent. Regardless of your profession or position in life, it is a real possibility that *you* could become the target of a bomb placed by terrorist or criminal elements currently operating with impunity within our borders and abroad.

Author Lawrence W. Myers has assembled a realistic, highly effective approach to addressing the three most common methods of assassination by explosives—vehicle, mail, and area-emplaced bombs. Drawing on his experiences as a counterterrorism specialist and bombing case files of the FBI Bomb Data Center, U.S. Secret Service, and U.S. Defense Department, Myers proposes a merciless, controversial tactic to use against those who attempt to utilize explosives for murder and terror: specially rigged (but easy-to-obtain) security devices that detonate the IED in the hands of the bomber, killing him.

Myers stresses other deterrents that, while not as extreme, are also highly effective. By implementing the canny countersurveillance techniques described herein, the lines become blurred between killer and victim, stalker and stalked. The object is to plant a seed of doubt in the minds of terrorists and criminals as to whether *they* have become the target in this deadly dance. Then, if they're foolish enough to try to emplace an IED against you or your property, they will die.

For information purposes only.

A PALADIN PRESS BOOK
ISBN 0-87364-608-8

COUNTERBOMB

PROTECTING YOURSELF AGAINST CAR, MAIL, AND AREA-EMPLACED BOMBS

LAWRENCE W. MYERS

PALADIN PRESS
BOULDER, COLORADO

Counterbomb:
Protecting Yourself against Car, Mail, and Area-Emplaced Bombs
Copyright © 1991 by Lawrence W. Myers

ISBN 0-87364-608-8
Printed in the United States of America

Published by Paladin Press, a division of
Paladin Enterprises, Inc., P.O. Box 1307,
Boulder, Colorado 80306, USA.
(303) 443-7250

Direct inquires and/or orders to the above address.

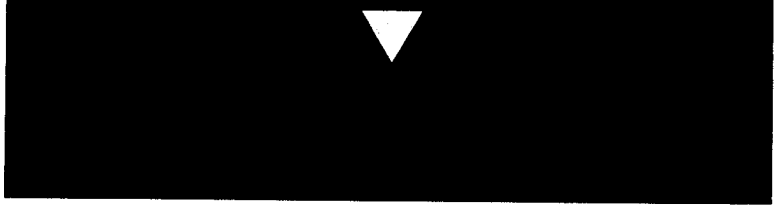
All rights reserved. Except for use in a review, no
portion of this book may be reproduced in any form
without the express written permission of the publisher.

Neither the author nor the publisher assumes
any responsibility for the use or misuse of
information contained in this book.

Illustrations by Mark Camden

CONTENTS

INTRODUCTION



Regardless of your profession or position in life, you could become targeted for a bomb attack. An improvised explosive device (IED) is simple to construct from readily available materials, and homemade bombs are being used for a number of criminal purposes these days.

There are a number of tactics and techniques you can adapt to effectively decrease the capability of an individual to deploy a bomb against you, your property, or those you are responsible to protect. This book is intended to provide the reader with an understanding of the nature of an IED threat in the context of preventing a target from becoming a victim.

This book does not explore the sociological causes or political ramifications of bombings. Like any other serious crime, the IED threat must be addressed, studied, and "managed" in a manner that is focused on prevention and deterrence, while at the same time attacking and interrupting individuals intent

on committing such violence.

Except in times of armed conflict, all bombings are criminal acts, and these attacks are becoming more common every year. According to the Federal Bureau of Investigation (FBI), the use of explosives as a murder weapon in the United States increased more than 430 percent between 1983 and 1988. A homicide victim is now more than twice as likely to have been killed by an explosive device than by intentional poisoning.[1] (See page 89 for Endnotes.)

There are dozens of military and paramilitary books available that describe a number of homemade IEDs that are more than capable of causing injury and death. By and large, these books are detailed and technically accurate. Many provide a number of substitutes for hard-to-get components, carefully stress safety procedures, and describe placement techniques that will cause maximum trauma to the target.

If you are serious about acquiring realistic survival skills in a high-threat situation, you may have some of these books in your library. You don't have to be an unproductive member of the "lunatic fringe" in order to have a real need for an understanding of IED technology. In fact, some of the best demolitions libraries I have encountered in my career have been in the squad rooms of small municipal police departments, on the bookshelves of private-security companies, and in the underground "situation rooms" of the well prepared.

The reality is that a bomb has a number of inherent characteristics that make it a common criminal tool. To construct an IED using indigenous materials from a local grocery or department store actually entails less risk to an assassin or terrorist

intent on killing a specific target than legally or covertly purchasing a firearm from either legitimate or underground sources. (In countries with severe restrictions on the availability of firearms, the IED is the primary tool of the insurgent, guerrilla, or terrorist.) A well-constructed and well-placed IED is also more likely to cause mortal trauma than several gunshot wounds. Additionally, the anonymous nature of an IED provides the perpetrator with a degree of isolation and distance from the scene of the attack. But perhaps the most significant aspect of IED use is that a semiskilled person can fabricate, test, and employ a bomb in a manner that is virtually impossible to predict or control.

Thus, availability, simplicity, and anonymity have always made the bomb a preferred weapon for a number of criminal and terrorist organizations. Regardless of the motivation involved, however, the majority of bombing attacks that cause injury or death are perpetrated by groups or individuals who have a specific reason for the specific use of explosives—the intent is almost universally to send a message of terror to those who survive the attack.

The criminal may wish to execute a potential witness or an aggressive competitor. He may also place an IED on or near the site of his criminal enterprise, as is the case in a growing number of instances involving illegal marijuana growers in the Pacific Northwest and the central Appalachian regions of the United States. Law-enforcement agencies across the country are now becoming more cognizant of the threat posed by these deadly booby-traps and assassination tools.

Your rural property or survival retreat may be illegally "shared" with any number of groups or

individuals who also have reason to maintain a low profile in a remote location. Moonshiners, marijuana farmers, clandestine drug producers, and paramilitary "wannabees" all have been known to employ IEDs to protect their illegal enterprises or to provide an early warning to intrusions.

As luck would have it, many of these sociopathic, semiliterate criminal types are often quite functionally inept at bomb making. Although it may be cruel to consider this fortunate, many amateur bomb makers seem to injure, maim, or kill only themselves while partaking in this somewhat unforgiving pastime.[2]

Because explosive devices tend to be nonselective in damage and casualties, many unintended injuries result from the placement and detonation of an IED. You or your loved ones may become victims of a bombing simply because of a peripheral association with the actual target or because of an accidental proximity to the blast zone.

This book is intended only to assist the reader in the recognition and detection of an IED threat. It is not intended to equip you with the skills of disarming an IED. Even highly skilled bomb technicians are injured or killed regularly in this extremely hazardous occupation.

Don't believe for a moment that you are skilled or clever enough to render safe any type of IED. Many bombs are intentionally designed to provide a deceptively simple appearance, when in fact they are engineered to "surprise" the overconfident. Nothing you have ever seen in movies or read in books can possibly equip you to address the threat of an explosion from an antipersonnel bomb.

On the other hand, you don't have to be a doctor

to prevent injury or disease, and you certainly don't have to be a bomb technician in order to take realistic measures to protect yourself, your family, and your property from the intentional placement of an explosive device. This book will focus on prevention and countermeasures to the IED placement mission, as well as address the threat posed by successful placement of a device despite your best efforts to discourage such activity.

Understanding the nature of these attacks is instrumental in countering the threat. The three most common methods of assassination by explosives—vehicular, mail, and area-emplaced bombs—are all based on bringing the target and the device as close together as possible in a "natural" and nonthreatening manner. This requires extensive preattack surveillance by the IED placement element. Yet such bombing attempts can be countered to a relatively high degree of efficiency with a few simple precautions.

The key to successful prevention of a bomb attack is the systematic denial of opportunity through threat assessment, "hardening" of potential target areas, and preestablished procedures for damage control. All countermeasures should be conducted with the intent of promoting a relaxed state of habitual alert while creating a clear psychological deterrent to those who attempt to observe your vulnerabilities as they conduct their preattack surveillance.

CHAPTER ONE

THREAT ASSESSMENT

Understanding the potential threat from a bomb attack involves making a brief personal assessment. If you are in a profession that is faced with an active opposition (e.g., military, security, or law enforcement), then you and/or your organization should have procedures in place to deal with any specific threat. A low profile is obviously the ideal security strategy if you are professionally predisposed to being in harm's way.

You don't have to be an undercover agent or a client of the U.S. federal witness protection program to face occupational risks from an IED threat. You alone should make an assessment of your "target potential" based on the nature and dangers associated with your occupation, interests, and affiliations.

Threat assessment is based primarily on good intelligence. This typically mundane task involves the study of your environment as well as your potential enemy. If you plan to set up a retreat in a remote section of mountainous terrain, it might be

wise to study the area beforehand, perhaps calling local law-enforcement personnel and/or the U.S. Forest Service for information on any illegal activity in the area. Although you may have purchased such isolated property with the intent of quietly arranging an emergency extraction location for yourself and your family, the location may already be illegally occupied for criminal purposes.

For example, as mentioned in the Introduction, marijuana cultivation in remote regions of the United States is becoming increasingly popular. In the past few years, I have encountered a variety of booby traps near national park trails on both coasts designed to protect marijuana plots from thieves. Many of these homemade protective devices are simple to detect and disarm; however, the increasing trend towards the use of IEDs with sophisticated detonation circuitry requires caution and alert environmental awareness.

Awareness of the local political scene is also important. Certain groups or individuals may not take kindly to your presence in a remote area. Sabotage of vehicles and roads in semideveloped wooded areas is becoming increasingly common as various political and criminal interests attempt to establish their "domain" in America's dwindling wilderness areas. Your legitimate possession of the real estate in question has no bearing on the behavior of certain environmental radicals or criminal elements.

Bomb attacks are extremely unpredictable events. The majority of the incidents that *are* prevented are identified and neutralized through good intelligence and a diligent focus on a few basic security procedures. The ability to predict all poten-

6-136 (Rev. 8-27-77)

FBI BOMB DATA CENTER

PLACE THIS CARD UNDER YOUR TELEPHONE

QUESTIONS TO ASK:

1. When is bomb going to explode?
2. Where is it right now?
3. What does it look like?
4. What kind of bomb is it?
5. What will cause it to explode?
6. Did you place the bomb?
7. Why?
8. What is your address?
9. What is your name?

EXACT WORDING OF THE THREAT:

_____

Sex of caller: _____ Race: _____

Age: _____ Length of call: _____

Number at which call is received:

_____

Time: _____ Date: __/__/__ (continued)

BOMB THREAT

CALLER'S VOICE:

__ Calm	__ Nasal
__ Angry	__ Stutter
__ Excited	__ Lisp
__ Slow	__ Raspy
__ Rapid	__ Deep
__ Soft	__ Ragged
__ Loud	__ Clearing throat
__ Laughter	__ Deep breathing
__ Crying	__ Cracking voice
__ Normal	__ Disguised
__ Distinct	__ Accent
__ Slurred	__ Familiar

__ Whispered

If voice is familiar, who did it sound like?

_____

_____

BACKGROUND SOUNDS:

__ Street noises	__ Factory machinery
__ Crockery	__ Animal noises
__ Voices	__ Clear
__ PA System	__ Static
__ Music	__ Local
__ House noises	__ Long distance
__ Motor	__ Booth
__ Office machinery	Other _____

THREAT LANGUAGE:

__ Well spoken (educated)	__ Incoherent
__ Foul	__ Taped
__ Irrational	__ Message read by threat maker

REMARKS: _____

_____

_____

_____

Report call immediately to:

_____.

Phone number _____.

Date __/__/__.

Name _____.

Position _____.

Phone number _____.

Figure 1. FBI Bomb Data Center card for bomb threats received over the telephone.

tial threat areas is impossible, yet an aggressive focus on the obvious can effectively limit risk to a more manageable level. This makes threat assessment the primary prevention and intelligence-tasking strategy.

ADDRESSING A COMMUNICATED BOMB THREAT

Another aspect of threat assessment is based on the procedural knowledge of and training for dealing with a specific bomb threat. If you are ever contacted by someone who clearly states that you are going to be a victim of a bomb attack, you are advised to take the threat very seriously.

Most bomb threats are communicated by telephone, and it is important to be prepared to receive and "process" them when they are made. Figure 1 is the standard FBI Bomb Data Center card issued by the U.S. government to military and federal offices for placement by the telephone. Federal policy states that these cards should be placed underneath every telephone in the building. From my experience, it seems more practical to mount these cards with tape or a thumbtack on a wall next to each telephone. This prevents the card from being used as scratch paper for quick phone messages by family members or employees. Ideally, the threat card should be by every phone on a clipboard with a pen attached to it.

Additionally, prominently posted bomb-threat cards provide a low-cost psychological deterrent. It cheaply communicates professional awareness to the bomb-placement or preattack surveillance operative. The FBI logo near every telephone in your business

establishment certainly does no harm, either.

Although it is obviously illegal, if you are in a profession where such threats are a common occurrence, it is not a bad idea to have the capability of instantly recording a telephone conversation. Low-cost cassette recorders and automatic recording devices can be obtained at any Radio Shack outlet. Sound judgment and discretion in the use of such devices can be most helpful to the investigative organization contacted after the threat is made.

Should you decide to take this approach in your threat assessment plan, some legal precautions are in order. I advise all clients to have the capability of recording a telephone threat, but I also advise them to never admit doing so. Modern technology has made this realistic and feasible. By using ordinary answering-machine cassette tapes in your recording device, you can record the telephone threat and provide the investigator with the tape. Stating that you "accidentally" left your answering machine on when the call came in allows both you and the investigator off the hook as far as the legal rights of the individual who communicated the threat over the phone are concerned.

From my experience, the intelligence value of such recordings is priceless. Of course, you should have a telephone answering machine on the premises, and you should be very cautious in your use of this technique. (Many newer models of answering machines have a recording feature attached. A switch allows you to record the call in progress even with the receiver picked up. This is perhaps the ideal solution.)[3]

The caller of a communicated bomb threat has only one motive in making the contact: regardless of

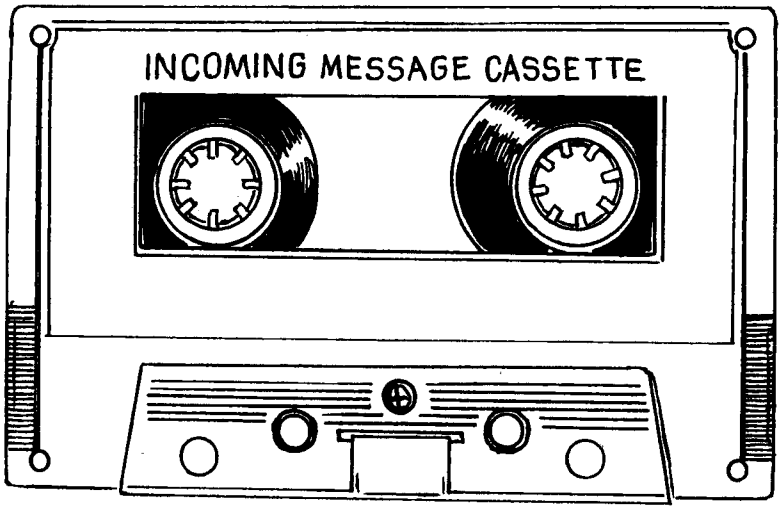


Figure 2. Telephone answering machines are available at many electronics stores such as Radio Shack. By recording a communicated bomb threat on a standard answering machine, you can claim to have "accidentally" left it on when the threat came in, capturing the caller's message on tape. This approach tends to limit liability and enhances the value of the recording as evidence.

whether an IED has been actually placed at your location, he or she feels a need to advise you of the threat. Consequently, all personnel should be knowledgeable on how to calmly deal with such a threat. They should be instructed to immediately begin filling out the bomb-threat card.

Typically, these calls are made from a pay telephone, and they are intentionally brief. Yet the longer the caller is kept on the line, the more intelligence can be collected. Training personnel to ask the caller to repeat the threat as soon as it is made is

helpful in getting the person to stay on the line for a few extra seconds. It also encourages them to elaborate. Simply sounding slightly confused and saying, "Excuse me, what did you say?" while reaching for pen and threat card is often instrumental in getting at least the first six or seven questions filled out.

The overwhelming majority of bomb-threat calls are false threats perpetrated by youngsters or as a means of harassment. Unfortunately, the legitimacy of the threat cannot be accurately determined based solely on the nature of the call. Therefore, the person who takes the call should never be sarcastic, abusive, or authoritative to the caller.

Since communicating a bomb threat is a federal offense, all personnel should be instructed to notify the police as soon as the call is terminated. The person receiving the call can also initiate a trace. In most parts of the United States, this procedure is now quite simple.

Initiating a Telephone Line Trace

If you are in a high-risk situation, it is suggested that you make arrangements with the telephone company to conduct traces on incoming calls in advance. File a "complaint" with your local telephone carrier stating that you have been receiving harassing or abusive calls from an anonymous person. Filing a false complaint with a corporation may seem somewhat unethical; however, most telephone companies charge a small monthly fee for a relatively new service designed to identify the person or persons making harassing or obscene telephone calls.

Basically, this service provides the customer with a means of initiating his own line trace. As soon as

the call is terminated, the customer makes note of the date and time the call was received and then dials a toll-free number. The call is generally routed to an "annoyance call center." The customer then dials a code number and his telephone number into the keypad. This initiates the trace. Finally, the customer states the nature and content of the call, which is recorded by an answering machine.

In many areas, a more instant service is available for the telephone customer. As soon as a harassing call comes in to the customer's phone, he or she simply waits for the caller to hang up. The service, known as "call trace," is initiated by dialing *57 (or 1 + 1 + 57 on a rotary dial phone), and the trace sequence is initiated. This service is currently available in most markets nationwide and is an excellent means of identifying the phone used for the threat.

Another unique service to consider is called "call return." As long as the call was made locally, it allows the recipient to immediately call the person back. This service has proven to be highly effective at dealing with the harassing caller. As soon as the person making the calls hangs up, his phone will ring. When he picks up, you tell him that you have already traced the calls back to him and will be prosecuting. This generally causes the caller a bit of anxiety, since it makes the caller believe that you have in fact traced the call very quickly. This service can be purchased in conjunction with the call trace for some creative threat-management possibilities. (To activate call return, you simply dial *69.)

This prearrangement permits a telephone trace regardless of the amount of time a caller spends on the line. The trace is no longer performed manually, and unlike television or movie depictions, the process

takes less than one second to identify the phone from which the call was made. (Since these new services are not very well-known, it is hoped that the reader will consider the advantages of not "advertising" this information. In fact, the new trace capabilities of the modern telephone system have resulted in the capture of several bombers, kidnappers, and extortionists over the past couple of years. Intentionally perpetuating the belief that a line trace takes several minutes to perform probably saves lives every year.)

Another useful approach to bomb-threat management employs a tape recorder, magnetic reed switch, and clipboards attached to the wall near each telephone. (A reed switch is a ferrous metal device enclosed in glass. A small thin reed moves to another reed inside the glass when exposed to a magnetic field, which closes an electrical circuit.) As the illustration shows, the clipboard has a magnet attached to the back of it. When the person receiving the call removes the clipboard from the wall, the tape recorder is automatically turned on. Using the clipboard with the automatic record function also allows you to keep the actual recording of the conversation private. No staff members need to know of its existence, and it is suggested that you keep this particular aspect of the procedure very quiet.

Threat procedures, the FBI Bomb Data Center card, and trace instructions are kept on the clipboard. This helps keep everything ready and organized. Having the clipboard posted on a wall encourages the operator to read the instructions and procedures occasionally to refresh his or her memory on handling a threat. This also tends to diminish anxiety to a degree when a threat is encountered.

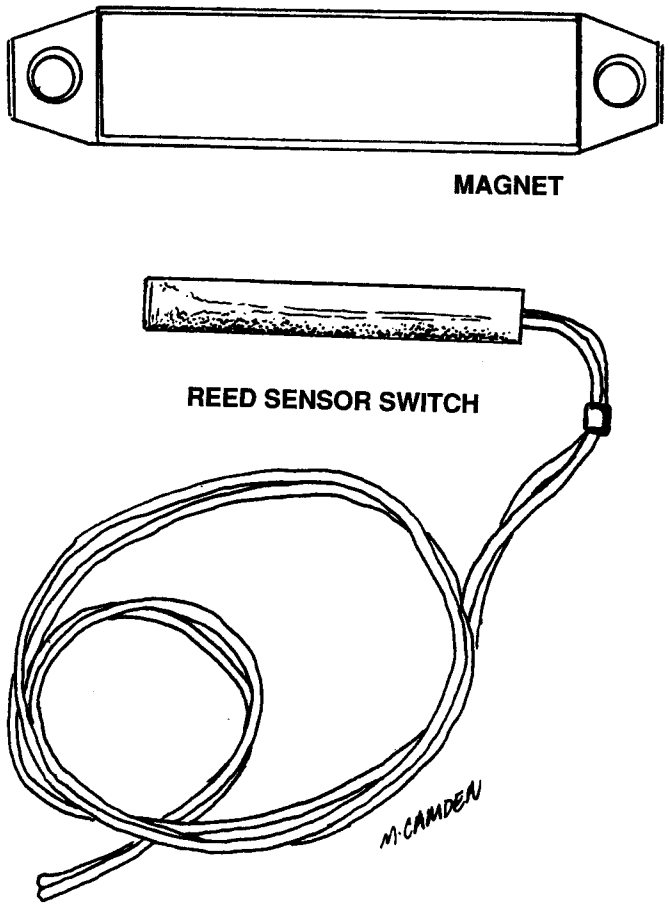


Figure 3. Frequently used in door and window perimeter security systems, an inexpensive magnetic reed switch has many other unique applications. By placing the magnet on the back of the clipboard and mounting the reed sensor switch on the wall directly behind it, the switch can be plugged into the remote jack of a tape recorder to begin the tape when the clipboard is removed from the wall.

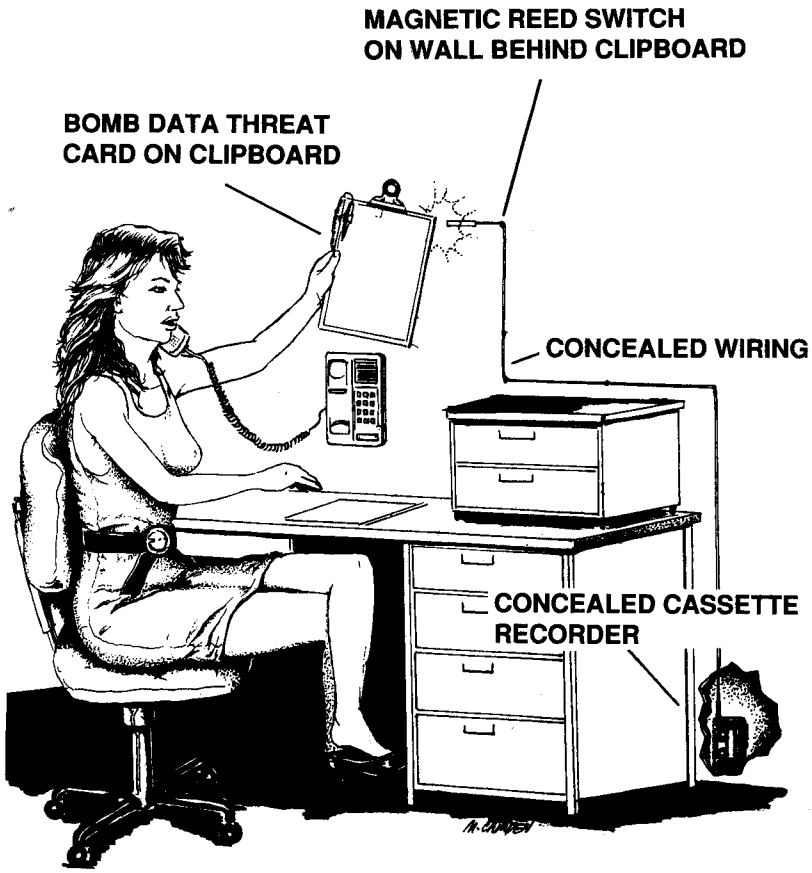


Figure 4. When a communicated threat is received, it can be processed by trained personnel. Bomb-threat procedures, FBI Bomb Data card, and trace instructions are kept on the clipboard along with a pen for quick, easy access.

Bomb Threat Procedures

1. Relax and stay calm.
2. Remove clipboard and ask person to repeat statement.
3. Calmly express concern for occupants of building. Do not sound sarcastic or authoritative to the caller. Do not threaten him or her in any way. Sound understanding and clearly ask that the person help you save lives.
4. Begin questioning individual using threat card. Immediately after call is terminated, fill in as many blanks as possible. Make notes on separate sheet of paper if necessary.
5. Do not panic. Do not discuss threat with anyone. Call supervisor at _____ and advise of the call.

Remember, if a threat is made, the person wishes to save lives. If you are calm and helpful to the caller, more details can be learned. Keep the caller on the line as long as possible. Most threats are not legitimate, but do not imply that you believe the caller is misleading you or that the call is a hoax. Show your concern for the safety of your fellow workers. Stay calm.

Figure 5. Bomb threat procedures.

You may rest assured that if you ever receive a legitimate bomb threat, having a neatly filled out Bomb Data Center card, a tape recording of the threat, and an initiated trace on the call will not only greatly impress the investigative agency tasked with the case, but the bomber is likely to have very serious legal and personal problems within hours.

CHAPTER TWO

BUILDING EVACUATION PROCEDURES

As soon as you have addressed the caller, it is time to carefully and methodically evacuate the area. If you are in charge of a large building full of people, the police will probably conduct the evac. If you are in a small or medium-size business, however, it is suggested that you slowly evacuate everyone in small groups of two or three. Send them out on an "errand" or give them the rest of the day off.

In most instances, it can be somewhat irresponsible (and frequently counterproductive) to advise personnel of the bomb threat. Your objective is to completely clear the building without causing panic or emotional duress. It is not only a burden on the stability of the employee (and bad for business) to "advertise" a bomb threat, doing so also tends to cause the evac to become disorderly and potentially dangerous. In fact, many large federal buildings are evacuated through use of the fire alarm, conducting the procedure as though it were a drill as opposed to an actual fire.

When outside the building, all personnel should clearly be advised of what to do. Again, sending them on errands or relieving them for the day avoids the well-documented "congregation effect," where groups of people stand around outside the building in small clusters. This is extremely foolish and should be carefully avoided because if the bomb threat is real, the caller may in fact have planted the device in a vehicle outside the building. When all the occupants are evacuated, the device may be command detonated to explode among these groups of people, causing massive injuries. This is, of course, a significant reason why mass evacuations such as fire drills are less useful means of evacuating a building than systematic individual release from the premises.

When considering evac planning strategies, a couple of other points are useful to remember. If the caller clearly indicates that the device is going to explode in a matter of minutes, immediately conduct a fire drill. These drills should be taken very seriously by all personnel, and should be a routine part of your business and home life. As you supervise the orderly evac, turn off the main circuit breaker in the building, shut off gas lines if possible[4], and open all windows and doors. These precautionary steps can greatly reduce peripheral damage and injury; if the explosion has a well-ventilated blast area, the fragmentation and shattering effect is greatly reduced.

Upon clearing the building, go outside and ensure that no one is standing within three hundred yards of the premises or congregating in any specific area. Perform a quick head count to confirm that everyone is out of the building.

It is also suggested that you casually observe the surrounding neighborhood. Many real bomb threats are made from a location where the caller can maintain visual observation of the intended target. Anyone standing near or around a pay phone should be noted, as well as anyone observed sitting in a vehicle or otherwise loitering in the area.

Like the archetypal deranged arsonist, the psychologically impaired bomber frequently observes the blast sequence from a safe distance in order to derive some sort of gratification from the experience. For the "mad bomber" type of personality, the actual explosion is often the primary motivation for assembling and placing an IED. He usually doesn't want to see anyone hurt or injured in the explosion; he simply wants to experience the "power" of making the blast occur.[5]

It is important to note that the experienced or highly trained professional may place a mock-up device in your area and then communicate a bomb threat in order to gauge your responses and take your "security pulse" prior to the actual placement mission. Such dry runs on a target are becoming almost tradecraft to the terrorist.

If you actually encounter a suspicious object while clearing the building or based on the specific details of the device communicated during the phone threat, *do not touch or get close to it!* If appropriate response personnel are going to take a while arriving at the scene, you may wish to take some quick containment precautions as described in the section on package bombs in Chapter 4. Generally, however, this is ill-advised and reckless. Your primary task is to clear the area of personnel, leaving doors and windows open as you calmly evacuate the building.

Accounting for all of your people and casually observing the neighborhood are much more useful and infinitely safer actions at this point.

Regardless of whether you are dealing with a hoax, a psychologically impaired person, or a determined criminal in a communicated bomb threat scenario, it is important to be completely prepared to address the threat in a manner which clearly emphasizes safety, protects lives and property, and possibly identifies or neutralizes the perpetrator, as well as intentionally create a clear psychological deterrent to the act itself.

It should be apparent that threat assessment essentially consists of planning and preparation. Collecting useful details regarding potential threat elements combined with procedural measures to address any specific threat diminishes anxiety for all personnel if a threat is received. This will result in the inability to terrorize and disrupt your organization with a mere threat of an IED placement.

HARDENING THE TARGET

Unfortunately, most bombing incidents do not involve a communicated threat prior to the blast. Therefore, the ability to safely address the real dangers involving a bomb attack will require more than basic intelligence and contingency planning. There are a number of precautionary measures that focus on becoming a "hard target." As in threat assessment, these measures emphasize prevention in a manner that subtly "advertises" a high degree of awareness.

It is almost impossible to overstate the effectiveness of presenting a psychological deterrent to

anyone considering you as a target for a bomb attack. All countermeasures employed to stop criminal activity tend to employ a highly visible force of personnel and technology. A number of law-enforcement tactics and techniques focus on presenting a convincing image of professional, capable, and prevention-oriented approaches to crime control.

The desired message to the public is that they are protected by skilled and dedicated professionals. The intent is also to present an image to the criminal or sociopathic person that this highly visible display of force may be a serious threat to their felonious enterprises. The mere presence of a fit-looking, uniformed officer tends to instill public confidence while creating paranoia among criminals. This same approach can be used to discourage someone planning to employ an IED against you or your property.

The person who is intent on getting you close to an IED must be extremely cognizant of your routine, the nature of your work, and your personal habits. The primary tool the bomber employs to gather this information is extensive preattack surveillance. He may operate alone or with accomplices to collect every detail about who you are, how you live, and what you do.

The purpose of the preattack surveillance is to reveal to the bomber exactly how, when, and where to place and detonate the IED. The more information the attacker can collect about you, the more likely he is to successfully emplace a device close to you. Good surveillance results in less explosive required and less emplacement risk, and greatly increases the probability of a successful attack.

Preattack surveillance is focused on making your life and your routine as comprehensive and predictable as possible to the bomb emplacement element. The most successful bombing attacks frequently indicate that the bomber had an almost uncanny ability to predict the behavior of the target. This may be as simple as addressing a package in a manner that makes the target feel safe opening it, such as by using a return address from a close friend or family member, or it may be as complex as knowing which rental car or hotel room the target has requested in a distant city.

Understanding the Stalker Syndrome

The intensity of preattack surveillance, which is conducted as a form of tradecraft by amateur and professional alike, can actually create a degree of psychological "bonding" between the attacker and his target. The bomber or assassin often begins to have a compulsive, one-way "relationship" with his intended target, becoming almost obsessed with every detail of his quarry.

This phenomenon is currently being studied very carefully by West German counterterrorist agencies. The preliminary indications are that, although the pattern appears to be somewhat obsessive-compulsive behavior, there is generally no identifiable psychosis evident in those individuals detained and studied. It is speculated that the bonding between the killer and the target is not based on the attacker having a psychiatric problem as much as it is on his or her exposure to the time-intensive, detail-oriented nature of surveillance operations in general.

The attacker tends to focus his surveillance operations on activities the target is likely to repeat

on a regular basis. While the restaurants and shops normally visited by the target are of use to the stalker, certain aspects of the target's life are even more lucrative subjects for intense study. Specifically, detailed surveillance often reveals personal habits and peculiarities about the target that are of great use to the attacker. An extramarital affair, a recreational drug habit, or an interest in a specific form of gambling or sports are all of more subtle intelligence value, because a person may occasionally alter his routine in visiting a dry cleaning establishment or perhaps have someone else do this or any other mundane task. On the other hand, the target is not likely to miss a private meeting with a mistress or alter a habitual drive into a seedy section of town to obtain drugs for his personal use. Once the diligent surveillance operative can establish a schedule pattern for those habits that provide the target with some sort of instant gratification, these movements become the primary focus of the surveillance.

When the target's behavior becomes a matter of prediction as opposed to study, an experienced operative will develop a very different mind-set. Interrogation of assassins who specialize in bomb placement or ambush scenarios frequently reveals that once the target is perceived to be predictable, the attacker is forced to concern himself with all the other variables relating to the mission (such as his own safety during the eventual IED placement) while still maintaining a detailed surveillance of his intended prey. What tends to occur is that the attacker reaches a point of "sensory overload" as he carefully ponders all the potential risks and variables involved with the mission. If the target

fails, just one time, to act in a manner that is now "expected" of him, the killer frequently believes that he must start from scratch in his detailed surveillance. This is generally the point where the obsessive attachment begins.

What is perhaps most notable regarding the compulsive behavior of preattack surveillance operatives is that although there appears to be a twisted sort of bonding in their minds, it has never been known to prevent the act of placing the IED in a manner most likely to kill the target. In fact, it appears that the closer the killer gets to his target emotionally, the stronger his or her resolve becomes to complete the mission.

It is probably of little practical use to explore the psychological implications of this stalker syndrome except to be cognizant of the fact that everything you normally do in your life may become the subject of a very diligent, marginally obsessive scrutiny by someone who is intent on making an unauthorized "appointment" between you and a bomb. Countersurveillance is the key element to avoiding this potentially deadly encounter.

CHAPTER THREE

COUNTER-SURVEILLANCE

In order for the target of intense surveillance to avoid providing intimate details of his behavior to a terrorist or criminal, it is vital to carefully consider and understand the basic mechanics of countersurveillance. A number of aspects of daily living can be altered to a small degree to deny an aggressive opposition the capacity to collect sensitive, useful information regarding habits, associations, and routines. Conceptually, the potential target must consider the nature of the image being projected, the use of deception to alter that image, and specific tactics designed to further discourage preattack surveillance. Countersurveillance includes both active and passive measures to cause difficulty to anyone attempting to collect sensitive details regarding your life and behavior.

PHASE ONE: IMAGE

Generally, it is conceded that any approach that

creates an image of diligent security tends to alter the thoughts and behavior of the criminal. Yet, unlike many forms of security protection, IED threat management requires that every countermeasure *be* real and not just "look" real. It can be a fatal error to emplace such "window dressing" as fake video cameras, untrained uniformed guards, or warning labels for nonexistent security devices in an area you intend to protect from a bomb attack.[6] History has demonstrated graphically that false security measures or untrained personnel manning high-tech sensory devices not only are essentially worthless, they also communicate a negligent image to the individuals most likely to conduct such an attack.

One major airline, for example, employs completely untrained dogs in high-visibility air terminals to give the impression that bomb-sniffing K-9 units are posted there twenty-four hours a day. This approach may have merit if the intent is simply to convince the flying public that they are protected, but it has absolutely no bearing on the level of protection against a real IED placement mission.

Experience has taught us that a professional terrorist will take nothing for granted in the careful study and observation of an area. If his preattack surveillance makes note of a certain security precaution, he will test the reliability of the countermeasure. In our example, the untrained dog would be quickly assessed and evaluated for what it was and not for what it appeared to be. Therefore, every protective measure and security precaution designed to demonstrate diligence should do so, if only for the peripheral benefit of preparing personnel to attack an IED threat or assist in reliably detecting one.

The fundamental difference between IED threat management and ordinary crime control is that, with an IED threat, the opposition fully intends to attempt the attack regardless of, or in spite of, every precaution taken to neutralize it. Consequently, every measure you employ to address the threat should be very real and professionally applied. Image is less important than substance. Countersurveillance is a case in point.

In order to avoid becoming a victim of a bomb attack, you have to avoid any identifiable pattern in your behavior. Since we are all creatures of habit, the essential element is to establish the "habit" of random, spontaneous movements and unpredictable execution of your normal daily routine.

This concept is relatively simple to understand, but it is almost impossible to effectively apply. Habitual behavior is an identifiable characteristic of the human condition. The relatively predictable, mundane motions we execute daily are frequently part of a long-established and often cherished personal routine. To alter the pattern in a significant way is difficult and frequently obvious to everyone around us.

The image of unpredictability is often perceived by most people as unreliability. In fact, a person whose behavior is difficult to identify in patterns and understandable routines tends to be perceived as being somewhat mentally unstable or emotionally stressed. In fact, if you think of a person you perceive as being the most strong-willed, formidable, and reliable ally you have, it is likely that this person is also one of the most predictable human beings you know.

To equate reliability with strength of character is

culturally characteristic of all Western civilizations. In order to avoid the appearance (and consequences) of being completely unpredictable and therefore unreliable, it is important to plan a pattern of random movement in a manner that maintains relationships and responsibilities, while giving the outward image of complete spontaneity.

The only way to appear truly random and unpredictable to anyone observing you is to carefully plan and execute your activities differently every day. This is actually fairly easy to do.

By simply maintaining a small schedule or appointment book, your personal and professional obligations can be met and the needs of your family attentively addressed in a manner that neither communicates your intentions nor establishes a pattern. This book should not only be used to track your appointments and obligations, but also to create a random sequence of activities for any given day.

This approach basically allows you to conduct your own surveillance on yourself. Use the appointment book to schedule and log your activities. Regularly study the notations and, within a few days, you will quickly detect any patterns and become aware of your vulnerabilities, as would anyone else. You, of course, can change the pattern as it is detected, intentionally altering your route, destination, and daily itinerary to be extremely deceptive. Be creative and make the task an interesting mental challenge.

Plan meetings at different locations. Always travel to and from each destination by a different route. Learn the back roads and side streets in every area. Don't become a recognized "regular" at any business or social establishment. Regularly change

dry cleaners, travel agents, grocery stores, and pharmacies. Learn all the branches for your bank and frequent each location in a random pattern.

You may find this approach to be somewhat confusing at first, but for many clients it is also quite enjoyable. It creates a potential for variety every day. Within a matter of months, this random pattern becomes a very difficult "habit" to break.

There are no hard and fast rules regarding random movement. The only constant in the execution of this behavior is to regularly ask yourself whenever you leave any point or arrive at any destination, "Does anyone but my family and closest friends know where I am going right now, when I will be back, or where I have just been?" You will find that it is often challenging yet relatively simple to consistently answer the above question with a "no."

Countersurveillance is not based on attempting to completely prevent your activities from being observed. Rather, it is the realistic understanding that if you are going to be carefully studied, the trained observer will conclude that your movements and whereabouts cannot be predicted for any given time in the future.

This simple approach will effectively frustrate the unstable person, and the "gifted amateur" will quickly be convinced that he lacks the resources to establish a pattern in your movements or behavior. More significantly, the professional surveillance operative will recognize your random pattern for exactly what it is. If he is persistent and diligent in his observation, he will recognize your behavior as intentional and realize that you are cognizant of the threat he poses to your security—and that you may

be waiting and watching for *him*. Unless he is operating completely on his own (known in the trade as a "singleton"), and is very experienced with "hard" targets, the attacker will at least subconsciously suspect that, while placing you under preattack surveillance, he may be in some sort of danger from something or someone he has not yet observed.

This induced paranoia can be very profound in some people. All bombers are criminals. They exploit the fact that few people are cognizant of the dangers associated with living normal, routine lives. Like the assassin or terrorist, the bomber has to feel tactically superior to his prey in order to execute his attack. When you effectively deny this advantage by communicating awareness, the stalker has to begin assessing his own safety before he is convinced that he can deny you yours. Not only does this tactic induce a degree of stress in the opposition, it also is conducive to the more substantive counter-surveillance measures that you may decide to employ.

PHASE TWO: DECEPTION

Once it is established by an aggressive opponent that your movements are difficult to track and predict and that you are aware of potential threats, the options available to the IED placement team are effectively reduced. At this point, the attack element must develop another means of collecting useful intelligence about your vulnerabilities. This is frequently accomplished through the use of deceptive contacts with the people closest to you.

If you run a small business, for instance, the attack element may call your office when they know

you are not in. They will ask to speak to you and, when told you are out, will attempt to elicit information about your location, destination, or schedule from your secretary or one of your employees. Although you may have a clearly stated company policy regarding the discussion of personal information over the telephone, experience indicates that regardless of what employees or friends are instructed not to talk about, they tend to openly discuss certain aspects of your life.

To prevent the people closest to you from providing information about your movements that could put your personal safety at risk, you can undertake a multilevel strategy. First and foremost, it is important that no personal information be available to nonessential personnel. Unless the employee or family member participates in planning your meetings, itinerary, or schedule, they should be excluded from knowledge of your activities.

From my experience, the willingness to exclude all nonessential associates from knowledge of one's activities is, without question, the hardest thing for a client to accept and apply. The protective element's request that release of information be made only on a need-to-know basis convinces many people that they cannot trust anyone, or that the protective element is insensitive to the feelings of their closest family members and associates. Thus, stressing security is difficult with most people because it restricts behavior or expression to a degree.

Nonetheless, it is important to emphasize to all employees and associates that your personal life should not be a topic of casual conversation. In many cases this request is reasonable, but it can also be unwise. By overstressing personal security, you

might convince people that they are not trusted, or that you are exceptionally paranoid. It is much better to simply keep all accurate information about yourself very "close hold." Never volunteer anything about your tastes or habits. Always seem non-committal and slightly distant to your employees and staff. This is a very professional management style that will generally eliminate personal matters from becoming a topic of discussion. You should also discourage inquiries from casual acquaintances about your movements and activities by never volunteering information, or by providing cues that your personal life is not a suitable topic of conversation.

Just as you have a close friend who is completely predictable, you probably know at least one person in your day-to-day life about whom you actually know very little. You don't know if the person is married, has children, or if they live in town or in the suburbs. You may not even know the type of car they drive, or their personal taste in food or entertainment.

If you see this person every day, or if you have regular business dealings with him or her, it may seem curious that you know so little about them. But it will also become obvious to you that this is because this person has never volunteered such information, and it actually is not relevant to your relationship.

More significantly, you have probably assumed a few things about this person that actually have no basis in fact. This is a common behavior characteristic of Americans in particular—if we don't know something about a person, we begin to make up a story about them based on our observations and what we hear. Forming an opinion or assessment of

someone based on superficial observations is common and quite natural.

In fact, what you think you know about a person whom you really don't know is almost universally wrong. Outward appearance, manner of speech, and general demeanor are seldom accurate measures of an individual's real self.

This particular aspect of the human condition is perhaps the most useful tool regarding interpersonal communications relating to security, as it can be exploited through the somewhat unethical but highly effective use of deception. If you share nothing with an associate or employee other than a few intentionally deceptive clues, then not only do they have absolutely nothing to accidentally "share" with a surveillance operative, but the information they think they have is incorrect and essentially worthless to the person out to do you harm. Thus, if a skilled operative goes so far as to attempt to learn about you through casual acquaintances, he will create a file of very conflicting observations. This will clearly communicate another message to the professional—that you are aware of the threat—which will further degrade his confidence in targeting you for attack.

Rest assured that if you do not tell associates about yourself, they will draw their own conclusions. You can "assist" them in making inaccurate conclusions, without the appearance of outright deception, through the liberal use of an age-old intelligence technique known as "litter."

Bumper stickers on your vehicle that relate to affiliations you actually have no connection with, pins and ties from schools you have never attended, matches from restaurants and bars you never

frequent—all of these are examples of good litter. If challenged by someone about this litter, shrug off the comment in a friendly way or even admit that you happened to have whatever it was they noticed for a completely different reason. Simply say it was a gift from a friend, or that you can't remember where it came from. Being considered slightly harebrained or disorganized is also a good message to send to a surveillant.

Litter collection, creative deception, and failure to participate in personal conversations are more practical ways to keep security-related information secret than by simply requesting it or expecting it from associates. This approach is friendly and actually fun once you get the hang of it.

Image and deception are somewhat passive countersurveillance techniques that are simple and unique to each individual in methods and application. You alone can formulate a personal protection plan that employs both to a degree that not only actively protects you from danger, but also has a significant psychological impact on the experienced stalker. These approaches to IED threat management also apply to basic personal security in general, providing protection from many other types of threat scenarios.

The third aspect of countersurveillance involves the tactics you can employ to make certain aspects of your life more difficult to observe by the trained operative. These tactics work well with image and deception to provide you with a realistic level of protection.

PHASE THREE: TACTICS

Once it becomes obvious that you are rather

difficult to study and predict, the surveillance operative is forced to resort to more active measures in order to collect essential details about you.

There are a number of vulnerable activities you probably participate in every day that require a small amount of alteration. This section will focus on specific tactics you can employ to make preattack surveillance extremely difficult for a skilled operative.

Identity

When conducting any type of personal business with a service industry, it is useful to provide a false name to the vendor. This is not illegal as long as you do so without the intent to commit fraud. This approach prevents a surveillant from pretending to be you and contacting a dry cleaner or restaurant to "verify" your service or reservations. He is also thwarted in using this particular personal or business relationship as part of his working file on your movements and activities. Finally, if he does not know which name you used, the operative is unable to predict when you will be at that location.

With this approach, you obviously are forced to pay cash for all services contracted, since a check would betray your deception. It is also important to keep track of receipts and claim checks, since you have no other means of proving you are the person contracting for the service. This tactic is particularly useful with time-intensive services such as dry cleaning, photo processing, watch or appliance repair, and so on.

Mailing Address

Control of all incoming mail is covered in Chapter 4. However, there is a tactic that you can use to

effectively screen all documents and packages based solely on the nature of the addressee.

You should have at least two separate mail drops established. One post office box is employed specifically for business and personal financial obligations. Virtually everyone who knows you or has business dealings with you uses this mail drop for correspondence. This is also the address you give to vendors when you give them a false name. By logging in your appointment book the name used when dealing with a specific vendor, you have a means of establishing how your address was obtained by any company sending junk mail or other offers.

By applying these two tactics, you will quickly learn that when you give a name and address for any service, not only does your transaction become a matter of record but your name is actually a salable commodity. Anywhere your name is sold or being used on a mailing list is a potentially high-risk situation. Avoid establishments that use your business relationship as a reference or an additional means of generating revenue.

Many businesses are aware that some of their customers do not take kindly to the distribution of their name and address to other vendors. They have a portion of the order form where the customer can specifically request that their name not be used in this manner. This is an excellent type of business to deal with occasionally.

Your second mailing address is given only to very close family members and friends, with the specific request that it not be shared with anyone. If you cannot expect this from the person, then they should receive your primary address only and have no knowledge of the second address.

This tactic is highly effective in screening for package or letter bombs. It also allows you to literally track any unsolicited materials back to their point of origin. This administrative screening process is highly conducive to the other measures covered under package bomb countermeasures.

Telephone Security

It is not only vital to restrict the information "shared" by employees and family members over the telephone, it is also critical that you take measures to deny a surveillant the use of your telephone as a means of access to you or your movements.

An unlisted telephone number in a fictitious name is a good start. Like every other service, there is no law requiring you to use your legal name when requesting telephone service. As long as you pay the bill on time (with a money order or bank draft), there is never a problem with using a fictitious name in the transaction. The telephone bills should be sent to your primary mail drop, and they should be carefully destroyed as soon as you have accounted for the calling record and paid the bill.

Avoiding telephone surveillance is more technical. One common method of modern phone tapping is the monitoring of cordless telephone conversations with a scanner radio. There are only ten possible pairs of radio frequencies allocated by the Federal Communications Commission (FCC) for use in a cordless telephone. While you may only be able to talk on one of these devices effectively for a few hundred feet from the base unit, a sensitive scanner can intercept both sides of your conversation from more than a mile away. If you have a cordless telephone, get rid of it. The conversations are not protected from eaves-

dropping or by any legal statute.

Likewise with a cellular telephone. The only time you can even marginally protect your conversations on a cellular phone is when you are traveling at high speed along a stretch of highway, where the frequency pair is likely to change every couple of minutes. Never talk on a cellular phone or any radio-link communications device if you can avoid doing so. If it does become necessary, be very conscious of what you say.[7]

Telephone traffic is very insecure. Always be aware that everything you say over the phone may be intercepted. Make all reservations or requests for services relating to your movements or itinerary in person or from a random pay phone.

Additionally, it is useful to have a means of screening all inbound telephone calls. A live answering service is a low-cost means of being remote yet accessible to those people with whom you need to be in contact. At your residence, an answering machine is useful to screen personal calls, and it eliminates the telephone from being used to accurately pinpoint your exact location at any given point in time. If you are known to answer your phone, it could be booby trapped and command detonated. Even law enforcement uses the telephone to pinpoint and verify a subject's location before kicking in his door to arrest him.

Document Control

There are certain written records which you keep that are very lucrative intelligence finds. It is important that you maintain strict control over all written materials pertaining to your personal life.

Your appointment book, credit card receipts,

address book, and personal correspondence from close friends or family members should be tightly controlled. Bank, insurance, and property records should also be secured from prying eyes.

Perhaps the most useful preattack surveillance strategy involves access to your garbage. There is nothing illegal about someone going through your trash, and this can reveal a lot about your personal habits and activities. Documents found in the trash, such as phone bills and empty envelopes from friends or family, are extremely useful to the stalker. They are dangerous bits of intelligence to lose control of, which is exactly what occurs when you throw them away.

A paper shredder is an excellent investment if there are a lot of documents that need to be regularly "neutralized" of their intelligence value. For personal use, however, a shredder is probably impractical. There are a couple of realistic alternatives.

If you get into the habit of sorting your refuse, a simple means of document control can be implemented. Any piece of mail, any bills, anything intimately related to your habits or associations can be destroyed by simply cutting it up with scissors and flushing it down the toilet. If a large amount of paper is involved, you might consider burning it in a fireplace or barbecue grill. Be conscious of the condition of the ash after burning, as the impact of the print wheel will still be readable if the ashes are not stirred.

If burning is not practical, another useful device for document destruction is an ordinary food blender. By filling the blender one third full of water and then placing the documents inside, you have a very

effective shredder that literally purees your documents in seconds to a completely unusable form. Using this simple technique, bulk amounts of paper can be safely poured into the toilet or used as a dense compost for light gardening chores. My clients are almost always amazed at how quickly and completely an ordinary blender can convert a paperback book or portion of a telephone directory into mush. This tactic is clean and fast, and it is actually more secure than most conventional shredders as a means of document destruction.

Document control also extends to text-processing media. Typewriter ribbons should be completely destroyed by burning or by pulling the ribbon out of the cartridge and shredding it. Single-use, multi-strike ribbons are very useful bits of refuse for the surveillance operative to find.

It is also of some merit to note when your trash collection truck normally arrives so you can effectively limit access to your refuse. Meeting the trash collector at his truck with your garbage is not a habit you want to be identified as doing consistently, but knowledge of exactly when the pickup occurs and even recognition of the individuals who normally conduct the collection is useful in countering the very real threat of a "garbage cover" being conducted against you.

COUNTERSURVEILLANCE CHECKLIST

The following checklist should provide the reader with a basic understanding of what to avoid and what to develop as a countersurveillance habit. Be creative and keep all countermeasures to yourself if possible.

Image

1. Never eat at the same restaurant twice in a row.
2. Never become a recognized regular at any drinking or entertainment establishment.
3. Always take a different route when returning from a trip.
4. Always use a variety of service contractors for repairs, cleaning, and personal care.
5. Avoid the habit of wearing an identifiable garment such as a certain coat or hat. Change clothing styles regularly.
6. Study your own pattern of movement regularly to detect and correct any identifiable routine.
7. Be aware of potential surveillance at all times. Observe your area for suspicious vehicles or individuals who appear to be watching you. Be particularly alert while arriving at and departing from a specific area.
8. Always project an alert image. Approach every new area with caution and obvious awareness.
9. Never telegraph your movements or intentions by traveling directly to a specific destination. Make your route spontaneous in timing and sequence.
10. Establish an intentionally unpredictable routine.

Deception

1. Never discuss your personal life or activities with associates or employees.
2. Be alert for unusual interest in your travel itinerary or location by seemingly casual conversation. Advise all employees to be suspicious

of such "innocent" inquiries, and to always report any such conversations to you.

3. Encourage speculation regarding your personal life and activities by never volunteering personal information while regularly providing intentionally deceptive clues.

4. Collect and casually display litter in a manner that indicates an affiliation or activity in which you actually never participate.

5. Develop deceptive behavior patterns. Regularly wave to complete strangers on the road, or hit your horn in greeting people you don't know. Occasionally make a quick U-turn for no apparent reason.

6. Visually "introduce" yourself to anyone who appears to be observing you. Say nothing—instead, simply stare for a second at the person's chin or forehead. Look as though you think you might recognize the person. This is an excellent way to spook a surveillant, and is also a very good exercise in observation.

7. When traveling on foot, make use of the environment. Observe the area through reflections in store windows and vehicle glass. Walk on the edge of the sidewalk, giving corners wide berth, and regularly scan the area as though you were looking for someone in particular.

8. If you regularly walk or jog as part of your fitness program, alter the time and route of your exercise constantly. Avoid times when the route is deserted. The best schedule is random times when the planned route is heavily traveled. Rush hour in a busy area is probably ideal.

9. Consider using a car pool that utilizes a number of different vehicles and routes. Schedule a

random pickup and departure time for all personnel.

10. Plan all activities to be random and/or deceptive in sequence and intent. Always be aware of what a surveillant may perceive about your movements.

Tactics

1. Always have an "inventory" of false names to provide a vendor or service business when asked. Make note of the control name used and track any peripheral effects of the transaction, such as inquiries or junk mail.

2. Avoid paying by credit card or check whenever possible. Use travelers checks or pay in cash.

3. Keep all records of transactions, financial dealings, medical or personal-care documents, and travel plans secure from unauthorized scrutiny.

4. Completely destroy all personal letters and documents once they are of no use.

5. Refuse to allow yourself or your family to be photographed for any reason. Carefully but politely avoid all media personnel.

6. Use random pay telephones as often as possible for placing orders for products or services. Always dial a public telephone quickly, in a manner that prevents observation of the numbers dialed.

7. Never use a cordless, cellular, or radio-linked telephone device, if at all possible.

8. Have an unlisted telephone number in a fictitious name. Have an answering service for your business, and give this number out when someone wants to contact you for a service or business transaction. Have an answering machine at home to screen all incoming telephone calls.

9. Carefully control personal résumés and biographical data. When applying for employment, recover both your résumé and job application if you are not hired.

10. Avoid any mail or telephone requests for personal information such as credit card offers, financial or personal service cards, and so on.

OVERVIEW

Your personal protection plan should be carefully and creatively designed to meet your specific needs and life-style. The intent and strategy should be known to no one but you. The most critical factor in countersurveillance is the ability to appear completely unpredictable in pattern of movement. Keep everything about yourself a private matter. Be deceptive, evasive, and difficult to describe or predict, and you will be an extremely "hard target" to surveil effectively.

CHAPTER FOUR

ACTIVE COUNTER-MEASURES

Good intelligence relating to specific threat areas, combined with countersurveillance, provides a high degree of protection from an IED threat. Yet hardening the target also entails the systematic reduction of opportunity through technical modifications to the customary target areas of an IED placement mission.

Specifically, a protection plan should address the threat of a vehicular placement, a letter or package bomb, and an area placement. The methods employed to deny opportunity through these media are focused primarily on the simple concept of access control.

TACTICAL OVERVIEW

Assassination by explosives is almost exclusively focused on the surreptitious placement of an IED in your vehicle, mail, or in an area where you are expected to be. Countersurveillance is useful in

addressing the threat of an IED placement to a degree, but there are certain active measures you can employ to further address the possibilities.

First, it should be pointed out that these countermeasures focus on the threat of an IED placement mission in a somewhat unconventional manner. The reader may not be particularly receptive to some of these approaches, because many of them are designed to cause injury or death to the IED placement element.

Whereas threat assessment provides a means of identifying many potential threats, and countersurveillance provides a measure of physical security and psychological deterrence to the IED threat, the specific approaches outlined in this chapter are intended to do two things. If the IED placement mission is attempted, the perpetrator must be prevented from successful completion of the act. Furthermore, from my experience, it seems "fair" to initiate countermeasures that employ technologies that place the person handling the IED at substantial risk of experiencing a premature detonation.

Specifically, warning systems that are currently available to protect various high-risk media (such as one's car or home) can create a high-output electromagnetic field designed to warn of the attempted penetration while simultaneously transmitting a powerful radio frequency (RF) pulse. This pulse will likely set off the detonation switching or electrical blasting cap inserted in the explosive compound of the IED. If an attempt is made to emplace an IED in an area where such countermeasures are installed (i.e., near you or your property), the IED will explode and kill the placement element.

This countermeasure has been successfully employed for several clients in Israel and Ireland. On one occasion, a placement was attempted in a client's vehicle that had this countermeasure installed, and the terrorist was killed when she attempted to put the device in the trunk. The group responsible for ordering the mission apparently believed that the premature detonation was the result of the young terrorist's mishandling of the device, because another attempt was made less than a year later on the client's new vehicle. Another premature detonation occurred, killing a 42-year-old male. Security forces speculated that he was tasked to attempt the placement mission because he was a more experienced operative

For obvious security reasons, it was never revealed that the probable cause of the detonations was the high-power electromagnetic environment created by the warning alarm on the vehicle.

It may be argued that alarms could be installed only to detect the placement attempt, perhaps causing the capture of the individual possessing the device. Intentionally designing circuitry that will likely injure or kill the placement element may be considered a cruel and unjustified response by civil libertarians.

It is conceded that this approach would deny the placement element "due process," but there are some very real validations for employing this countermeasure. The most obvious is that if an individual dies in the process of attempting to kill you, he will not pose any further threat to anyone. Further, the nature of the detonation causes those conspirators who survive the experience to severely question the capabilities of their devices, as well as the skill of

their placement people. Of most significance is the fact that this approach actively discourages further attempts by continuously killing those who try. It also causes the terrorist organization to experience a small "recruiting problem" in getting someone to attempt another placement mission. In the long run, this admittedly brutal countermeasure probably saves lives.

VEHICULAR PROTECTION

Your personal vehicle offers a number of tactical advantages to the placement element. Unless the vehicle is always kept in a secure garage or under diligent security, this medium is probably the preferred means of placement.

Although it is generally conceded that an automobile is difficult to protect continuously from tampering or IED placement, there are many important reasons to make your vehicle the hardest potential target in your protection plan.

The placement of an IED in a vehicle is an extremely popular assassination technique. A small explosion inside the confined area of an automobile's passenger compartment almost always results in mortal trauma. The vehicle contains the blast to a degree that causes more fragmentation and secondary blast exposure to the occupants.

The vehicle also places a number of detonation switching possibilities at the disposal of the bomber. The ignition system, brake lights, headlights, and many "comfort options" on an automobile can be accessed without entry to the passenger compartment, and can be wired to detonate the IED when the target performs a specific maneuver.

For example, in an actual incident that occurred in 1979, the IED placement element knew that the target frequented a local bar with a somewhat well-lit parking lot. The target was cognizant of the risk of an IED threat, and his patterns and movements were random and difficult to predict. He generally parked near the door, and the vehicle had an alarm system installed, which was "tested" by the placement element several weeks earlier. A loud siren went off if the vehicle was bumped or entry to the trunk, engine compartment, or passenger area was attempted.

The placement element was advised by surveillance that the target was at the bar one night. One operative parked his nondescript older vehicle next to the target vehicle and opened up the hood on his own car, appearing to do some sort of work on it. He removed the air filter cover and accidentally dropped the wing nut on the ground between the two cars. After quickly scanning the area, he dropped down and crawled close to the target vehicle with a small flashlight. He had the wing nut in his hand so if he were challenged by anyone, he could simply claim that he dropped it while trying to fix his vehicle in the dark.

The operative took a small, prewired IED from his pocket and attached it magnetically to the underside of the vehicle between the fuel tank and chassis. He ran a leg wire (those wires running directly from the blasting cap to the switching circuitry) up to the headlight plug and connected an alligator clip to the high-beam connection. He grounded out the other leg wire somewhere on the chassis. Since he had carefully practiced on a duplicate vehicle in total darkness, this entire

maneuver took less than one minute. The operative got up, placed the "missing" wing nut on the air filter of his car, closed the hood, and drove away.

About an hour later, the target got in his car and pulled out of the parking lot and onto the main roadway. After gaining speed, he turned on the high beams to see down the dark, deserted highway. The charge exploded, causing the gas tank to explode and the vehicle to crash at high speed. Since the device was magnetically attached, it fell off during detonation, along with the wiring. The alcohol in the target's blood was blamed for the crash, and the crash was attributed to be the cause of the fuel tank explosion.

This IED placement did not require access to the inside of the vehicle, and it was practiced enough to avoid setting off the vibration sensory security system during placement. The target was expected to be alone on the road when he turned on his high beams, so there were no witnesses to describe the sequence of events that occurred during the crash. Also, the high-beam connection was chosen because the placement element predicted that the target would be traveling fast on a low-visibility section of road, where control of the vehicle was less likely.

Wiring a car from the outside (i.e., easily accessed areas) is the real nature of IED placement on a vehicle. It is very unlikely that the detonation will occur when the vehicle ignition is switched on. It is much easier to utilize those points on the target vehicle that can be penetrated from underneath the car, causing a different sequence of events to occur rather than ignition.

The still partially classified details of the above incident indicate that it was done for criminal rather

than terrorist or political reasons. Had a diligent patrol officer not returned to the scene the following day to look for and make note of the skid marks on the highway, no one ever would have noticed the darkened section of road where the unburned particle traces from the explosion were found with small fragments of metal imbedded into the asphalt. (Eventually the attack was ruled a homicide, although the crime has never been solved.)

The real lesson to be learned here extends beyond the fact that the victim was predictable or that he chose to become a regular at a local watering hole. The investigation revealed that the security system installed on the victim's car had to be adjusted several times because the vibration sensor caused the alarm to sound at the slightest touch by a pedestrian. This caused the victim's neighbors to complain of being awakened at all hours of the night every time anyone passed by and touched his car. According to the report, the alarm even went off on occasion when large trucks drove by the vehicle. Consequently, the victim had taken his car back to the alarm company to have the sensitivity of the vibration sensors adjusted to avoid such false alarms.

The ideal auto security system should provide a means of notifying the vehicle owner that a possible tampering is occurring as well as a means of frightening off the petty criminal. This can be accomplished through the use of a car alarm pager system in conjunction with a siren.

The sensory environment of the vehicular security system should cover three separate areas: vibration, electrical tampering, and attempted entry. The vibration sensors, your first line of defense in a

vehicle protection plan, are connected only to the alarm pager, while the electrical and entry sensors are connected to both the pager and the loudest alarm siren you can find.

Whenever possible, the vehicle should be parked within sight of your location. This allows you to observe the area from a distance after being warned by pager of any tampering. Habitually parking your vehicle in a well-lit area is an excellent deterrent to tampering as well.

Readers with any experience with explosive devices are probably grinning slightly at this point, because the peripheral benefit of the auto alarm pager in IED threat management should be obvious.

Electrical blasting caps are extremely sensitive to electromagnetic energy. Lightning and radio waves pose a particularly dangerous threat to those using these sensitive devices. Military-trained demo personnel know not to come within fifty meters of a hand-held two-way radio when handling electrical blasting caps. Additionally, using electrical blasting caps near any high-voltage tower or radio station antenna is very dangerous.

An ordinary car alarm pager system broadcasts a strong RF pulse in the eleven-meter HF (high frequency) range at a maximum output power of four watts. A blasting cap should not be within thirty meters of the antenna of such a device unless it is completely encased in a shielded metal container.

The IED will most likely employ an electrical initiation sequence. In fact, it is frequently the leg wires that are connected to the vehicle switching system, causing the blast to occur when the victim is occupying the vehicle. This universal design characteristic of a vehicular IED placement mission

can be exploited. The blasting cap's leg wires function as an antenna to a degree when the operative attempts to connect them to the vehicle. If the vibration sensor is set on maximum sensitivity, it is virtually impossible to touch the vehicle without setting the sensor off. Of course, the sensor switching initiates the alarm pager, which will generate the RF field and notify the owner's receiver (within a two-mile radius) that tampering is occurring.

This RF field will set off the electrical blasting cap, and if it is preassembled and inserted into the explosive for a quick placement mission, the charge will most likely explode in the hands of the bomber. A "clever" bomber will be underneath your vehicle when this premature detonation occurs; this not only virtually guarantees his immediate death, but somewhat contains the blast under the vehicle, thus lowering any damage to nearby vehicles or structures. Of course, the bomber will want to attempt his placement while no one is around, which also allows this countermeasure to be used with confidence that the bomber is the only person likely to be the victim of the blast.

A few technical notes may be helpful regarding this deadly countermeasure. First, the standard industrial and military electrical blasting cap is known as a number 6 in military nomenclature, or a J1 in commercial applications. The electrical resistance of the blasting cap is 2 ohms, and it requires 1.5 amperes, typically for one second, to set it off.

An unscientific testing of a batch of these caps revealed that they will in fact fire with only .5 amperes, or one-third of their actual specified requirements. Additionally, these caps will fire when

within three yards of a transmitting antenna of the type employed in an auto alarm pager.

Terrorists also employ electrical blasting caps. The standard cap used by various groups happens to be the one most widely distributed among them throughout the Middle East and Europe—the Soviet-made EDP, or EDP-r electrical blasting cap. It has a resistance of 2.5 ohms and requires only 500 milliamperes (or one-half ampere) to fire. This makes the Soviet cap extremely sensitive to RF. It is, in fact, well over twice as likely to fire prematurely when exposed to equal amounts of RF as compared to the U.S.-made number 6.

If the bomb placement element has employed Soviet-type blasting caps in his IED, the auto alarm pager will very likely cause premature detonation.

Auto alarm pagers are inexpensive and readily available at Radio Shack outlets, department stores, and firms dealing in auto security systems. These devices typically use the vehicle's radio antenna to transmit the alarm pulse. The vehicle chassis serves as a ground plane for the transmission, meaning that the IED will detonate anywhere near the vehicle, not just in proximity to the antenna.

In order to virtually guarantee a premature detonation as well as greatly increase the effective range of the alarm pager, many clients attach a small linear amplifier to the pager to increase the output range. A standard CB radio linear amplifier, although illegal, is inexpensive to purchase or construct from a small amount of parts. If you employ a linear amplifier, you can test its efficiency by checking out the range capabilities of your pager. Testing the nature of the massive RF pulse of the device can be accomplished by driving your vehicle

close to a grocery store that has automatic door openers installed at the entrance. When the pager transmits, it will cause the sensors of the doors to switch on, opening them.

Don't hesitate to purchase a working linear amplifier from the black market in your neighborhood. A local CB radio operator can assist you in obtaining this inexpensive device, frequently termed a "foot warmer" in CB slang. If the device is illegal, it will probably have a high output of harmonic noise. This is definitely not wanted in standard radio applications; however, as a means of causing a premature detonation, the higher spurious harmonic output the device generates, the better.

A good linear amplifier connected to your alarm pager will not only allow your vehicle alarm to alert you from more than a hundred miles away, it will also set off a blasting cap from an impressive distance. If you have access to electrical blasting caps, you will be amazed at the distance from which a 100-watt RF pulse will cause the cap to explode.

An alarm pager can also be hooked up to sensors around your residence or business to accomplish the same effect. Of primary consideration is the potential risk of causing the charge to explode near innocent persons. Be very careful when using this deadly technique in populated areas or near your own home or business.

(For more detailed information regarding auto alarm pagers, refer to my book, *Improvised Radio Detonation Techniques*, available from Paladin Press.)

You can harden a vehicle with a good security system on your own or with the assistance of a good auto security firm. A lot of vibration sensors should

be used on the installation, and they should connect only to the pager alarm and *not* to the siren. The vibration sensors should be set for maximum sensitivity.

There are other areas to consider for vehicular protection. A locking gas cap and good locks on both the hood and trunk compartments are critical. You might also want to consider a performance upgrade on the underside of your car, where a fiberglass or sheet metal cover is placed under the chassis to provide better aerodynamics. This expensive modification eventually pays for itself through better gas mileage, and it denies access to the underside of your vehicle's transmission, exhaust, and fuel systems.

Another important countermeasure that is simple to install is a half-inch chicken wire barrier inside the exhaust pipe. This can be as simple as stuffing a wad of chicken wire into the exhaust outlet, or you can purchase an exhaust extender fitting from an auto supply store and do a custom job. The two considerations for this highly effective countermeasure are that the screen mesh should not impede the exhaust flow by being too dense, and it should not be visible or easily removed from the exhaust pipe.

This simple countermeasure not only prevents an IED from being placed inside the exhaust pipe, it also prevents the potentially deadly "prank" of putting a shotgun shell inside the exhaust, which is described in several of the "revenge" books that have become so popular.

The simple screen mesh denies access, which is the primary function of a countermeasure. Other access control tactics to consider for vehicular

security are based on good perimeter security where the vehicle is normally parked. The popular infrared floodlight devices available at many department stores are useful in this application. The sensor head and floodlight sockets are mounted so the sensor is focused on the vehicle's normal parking place. This protects both the vehicle and the surrounding area from intrusion. (Of course, the infrared sensor can also switch on other devices, such as an internal warning buzzer or an auto alarm pager.)

Access control should also provide an early warning indicator to successful penetrations. This is very important to vehicular protection in particular. One very useful approach is simple cleanliness.

If the outside of the vehicle is kept immaculately clean and waxed, any signs of "probing" will be easier to detect. If the underside of the vehicle is given a good outer body, rustproof undercoating seal and is regularly steam cleaned, any tampering in that area will be much easier to recognize. If the interior of the vehicle is regularly cleaned and vacuumed and the dashboard wiped and sprayed with a protectant, it is almost impossible to enter and quickly emplace a device without leaving a telltale sign of entry. Have nothing under the seats or on the floor. Keep your trunk in the same condition. The more attention you pay to detailed cleaning and maintenance, the more likely you will detect intrusion or alteration if something is out of place on the vehicle.

Another area where an IED is likely to be placed or the detonation switching wire connected is under the hood. Therefore, a hood lock is an excellent investment. Additionally, if you are going to leave your vehicle unattended for any period of time, it is a

good idea to carefully inspect it prior to starting the ignition or moving it.

A careful search of the vehicle takes about an hour if you are unfamiliar with it and only semitrained. Yet a detailed search is not something you necessarily want to do because it is becoming increasingly likely that any IED placed on a vehicle will have antitampering circuitry installed. Any tampering that may occur during a detailed search will cause a sophisticated IED to explode. A realistic alternative is to regularly perform a visual inspection of the vehicle for signs of tampering.

One useful way to do this quickly is by regularly taking photographs of the engine compartment after the vehicle is serviced or the engine is steam cleaned. With a few photos of the engine compartment in hand, anything new or out of place will

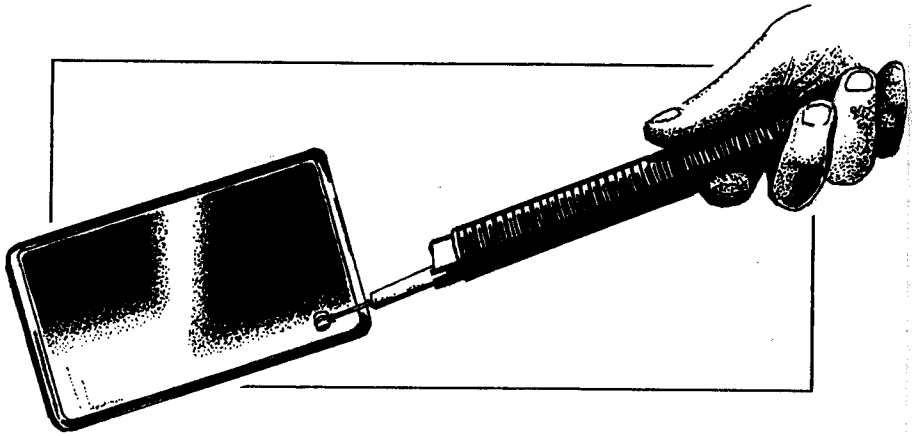


Figure 6. This inspection mirror is manufactured in Great Britain and issued to members of Parliament. It has a built-in flashlight, and the handle telescopes out to almost three feet. Similar devices are sold in several U.S. catalogs offering security equipment, as well as throughout Europe and the Middle East.

become quickly obvious to even an inexperienced observer.

A small inspection mirror, available in any electronics parts outlet, and a penlight will allow you to quickly inspect the underside of the vehicle as well. When the car is being serviced on a hydraulic jack, you may seem somewhat strange to the mechanic, but he will usually allow you to enter the service bay to take a few quick photos of the car's underside. Take these photos at right angles to the vehicle in a manner that will allow you to compare them to the mirror image during your quick inspection. Locking hub caps and a good undercoat seal in the wheel wells facilitate quick inspection and address the tampering and threat risk quite well.

Other basics to consider in vehicular protection are to always keep the vehicle locked, no matter how long you will be out of it. Regularly change mechanics, using only well-established chain service outlets, or learn to perform basic service by yourself. Always have the fuel tank full; never let it go under 50 percent capacity. This is not only a good habit from an emergency extraction point of view, but a full gas tank has much lower explosive potential than a partially or even completely empty one. Get into the habit of regularly topping off your fuel tank, checking the oil, and so on while comparing what you see to the most recent photo, and avoid any pattern in service, refueling, or cleaning-outlet use.

As you can see, the ideal approach to vehicular security is based on personal participation in regular care and maintenance of the vehicle. This tends to make the owner more aware of any tampering as well as keep the vehicle in extremely reliable condition.

good idea to carefully inspect it prior to starting the ignition or moving it.

A careful search of the vehicle takes about an hour if you are unfamiliar with it and only semitrained. Yet a detailed search is not something you necessarily want to do because it is becoming increasingly likely that any IED placed on a vehicle will have antitampering circuitry installed. Any tampering that may occur during a detailed search will cause a sophisticated IED to explode. A realistic alternative is to regularly perform a visual inspection of the vehicle for signs of tampering.

One useful way to do this quickly is by regularly taking photographs of the engine compartment after the vehicle is serviced or the engine is steam cleaned. With a few photos of the engine compartment in hand, anything new or out of place will

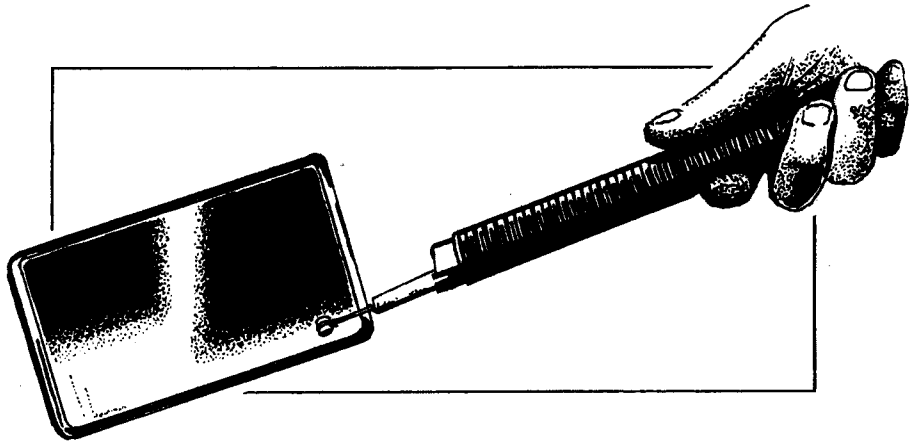


Figure 6. This inspection mirror is manufactured in Great Britain and issued to members of Parliament. It has a built-in flashlight, and the handle telescopes out to almost three feet. Similar devices are sold in several U.S. catalogs offering security equipment, as well as throughout Europe and the Middle East.

become quickly obvious to even an inexperienced observer.

A small inspection mirror, available in any electronics parts outlet, and a penlight will allow you to quickly inspect the underside of the vehicle as well. When the car is being serviced on a hydraulic jack, you may seem somewhat strange to the mechanic, but he will usually allow you to enter the service bay to take a few quick photos of the car's underside. Take these photos at right angles to the vehicle in a manner that will allow you to compare them to the mirror image during your quick inspection. Locking hub caps and a good undercoat seal in the wheel wells facilitate quick inspection and address the tampering and threat risk quite well.

Other basics to consider in vehicular protection are to always keep the vehicle locked, no matter how long you will be out of it. Regularly change mechanics, using only well-established chain service outlets, or learn to perform basic service by yourself. Always have the fuel tank full; never let it go under 50 percent capacity. This is not only a good habit from an emergency extraction point of view, but a full gas tank has much lower explosive potential than a partially or even completely empty one. Get into the habit of regularly topping off your fuel tank, checking the oil, and so on while comparing what you see to the most recent photo, and avoid any pattern in service, refueling, or cleaning-outlet use.

As you can see, the ideal approach to vehicular security is based on personal participation in regular care and maintenance of the vehicle. This tends to make the owner more aware of any tampering as well as keep the vehicle in extremely reliable condition.

When considering a temporary parking location, it is always a good idea to observe the area surrounding the vehicle prior to parking. It should be well lit and on a well-traveled route. Parking close to your destination is a good rule of thumb, but the physical security of the area is equally important.

Get into the habit of observing the ground close to the vehicle, particularly if you park on soft earth or gravel. Make quick note of any footprints or markings nearby where someone may have slid under the car while it was unattended. This habit is relatively easy to develop, and after several intentional, close studies of the area, an instinctive ability to detect activity develops.

Vehicular security is a very serious IED threat-management technique. Use your imagination and creativity in formulating a personal plan to keep your vehicle inaccessible and difficult to penetrate.

PACKAGE AND LETTER BOMB PROTECTION

In order for a bomber to get you to personally open an unsolicited letter or package, he must somehow cause you to believe the contents are of interest or use to you. This interest must be created while eliminating the fear of potential harm by inducing a degree of familiarity.

The most common method employed to create a nonthreatening interest is deceptive labeling. The package may come on or before a significant date, such as an anniversary or birthday, or it may come around the Christmas holidays. A "mail cover" or "trash cover" may have been placed on you, providing the bomber with intimate details of your

Figure 7. Vehicle security protection against bomb placement, theft, vandalism, and tampering.

correspondence and associates. Consequently, the return addressee will often be someone you know intimately, such as a close relative or old friend. In fact, the package containing the bomb may have actually been sent to you from a legitimate source—it may have been intercepted, carefully opened, booby-trapped with an IED, and then placed back in your mailbox. In recent bomb attacks using mail or packages, the actual packaging or handwriting of legitimate correspondents were typically employed to further increase the victim's confidence.

Monitoring your telephone conversations extends an incredible number of possibilities to the diligent IED placement operative. If a bomber has access to your telephone conversations for any period of time, he will eventually learn of an order for a product placed over the telephone. Of course, when you receive the package with the return address of the company, you will open it without hesitation.

An alert surveillant can exploit any piece of intelligence relating to your expectation of a package or document or your likelihood of considering a certain item to be nonthreatening. If the preattack element discovers that you occasionally order a pizza delivered to your residence, he can easily have everything available to deliver an IED package to your doorstep after canceling your legitimate order.

Countersurveillance is a critical area in addressing a mail bomb attack. Your vulnerability to such a bomb is extremely high. A delivered IED is considered by terrorists, criminals, and even some "action-oriented" foreign intelligence agencies as an efficient and useful tool for assassination.

Understanding the Threat

Many businesses have means to electronically screen packages for explosives or suspicious contents. U.S. federal facilities employ x-ray devices as well as more advanced technologies to address the threat. This is effective to a degree, but there are a growing number of cases where the package or letter IED was able to pass through the security screening, giving the victim a false sense of security just prior to the blast.

Understanding the proper countermeasures requires that a few common misconceptions regarding package or letter bombs be addressed. First, it is not likely that the characteristic "feel" or image of the outside packaging will betray the contents of a delivered IED. Although there are several warning indicators for a suspicious letter or package, there is no longer any infallibly identifiable characteristic. Mail IEDs do not make noise, emit strange odors, or have a characteristic weight, size, or density.

A letter bomb capable of mortal trauma can be constructed by a semitrained individual from a number of explosive materials. One increasingly popular charge for letter bomb fabrication is ordinary TNT.

TNT (trinitrotoluene) is used for a number of military and industrial applications. It comes packaged in quarter-, half-, and one-pound cylindrical or rectangular containers. A cap well for insertion of a blasting cap and metal end caps make this stable, waterproof compound suitable for a number of military and civilian demolition applications.

TNT is popular for letter bombs because of its

extremely high rate of detonation (6,900 meters per second, 22,600 feet per second) as well as an unusual characteristic when it's detonated in an enclosed room. When TNT explodes in a poorly ventilated area, an extremely toxic gas is formed. If the victim does not die from the initial trauma of the blast, the toxic gas environment will quickly kill him.

By carefully removing the outside packaging, TNT can be powdered and lightly glued to a sheet of ordinary paper for use in a letter bomb that weighs little more than a few grams. Micro detonators that are smaller than the typical metal hasp on a manila envelope are now available on the open arms market.

Other types of letter bombs are nothing more than ordinary paper impregnated with some sort of incendiary or explosive compound. In my book *Smart Bombs*, available from Paladin Press, I cover a simple-to-construct letter bomb that employs ordinary flash paper and a chemical initiation sequence.

A package-size IED can contain any number of compounds and detonation switching circuits. It may be carefully designed to defeat x-ray or "sniffer"-type bomb detection devices. Again, the weight and balance of a package IED have no identifiable characteristics.

The fact is that there is no reliable image or sensor technology capable of effectively screening a package or letter for explosives. A constant reliance on sophisticated gadgetry by government and industry to address this threat is perhaps the most useful strategy for a determined criminal or terrorist to exploit.

There are, however, a number of promising

detection technologies being developed. Some may eventually allow the average citizen or business to effectively screen large amounts of incoming packages and correspondence for explosives. Until that day arrives, a more realistic approach to this increasingly common IED threat must be initiated.

Access Control Procedures

The most important aspect of letter and package bomb prevention is access control. Denial of the attack element's physical access to your mail prevents preattack surveillance regarding who normally sends what to your address and addresses the threat of intercept and replacement.

The first critical countermeasure is to deny anyone the ability to handle your correspondence other than you and postal employees. This requires that you arrange to have your mail held at the post office in a post office box until you or someone you trust can pick it up. If you can possibly avoid it, never allow any mail to be sent to your residence or business directly.

The post office box provides a high degree of security from mail-cover surveillance or tampering. It also allows you to inspect specific letters or packages prior to actually having them in your home or business. All U.S. post offices have preestablished procedures for handling a suspicious letter or package, as well as equipment generally on-site to address the danger of an IED package.

A word of advice regarding use of the post office box: have someone other than yourself regularly pick up the mail. This should be done at random times by a trusted employee or family member. The person picking up the mail should know what normally is

INBOUND PACKAGE LOG SHEET

Source & Contact	Date Shipped	Date Expected	Item Description	Estimated Weight	Method of Delivery	Date In

Figure 8. Sample log sheet for inbound packages.

expected to be delivered, as well as what obviously is not. Anything suspicious or not wanted should be discarded with minimal handling or should never be accepted in the first place.

Another important consideration is to have the person always carry a small bag or canvas sack in which to conceal the mail immediately after removing it from the box. This defeats the old intelligence tactic of sending out a bright-colored or oversized envelope to a target's P.O. box in order to identify who is picking up the mail or determine the physical address of the target by following the courier.

It is important to continuously change the pickup schedule as well as the person performing the pickup on a frequent but random basis. Mail should be placed directly into a bag and brought directly to you. You should then carefully inspect each item again and discard anything unsolicited or unusual. Refer to the checklist at the end of this chapter for a few general guidelines.

Package control requires the use of simple log sheets. Any time a business or family member intends to send you a package, it is important that they advise you in advance and that a written record of the shipment be made. This inbound log sheet should contain the date any product was ordered, a description and estimated weight of the product, expected date of receipt, and any identifiable packaging information, such as return address and company logo, as well as when the package is received.

Many clients prefer to develop a coding system for personal and business package shipments. All orders to a business vendor should contain an

identifier code in your address to verify the package shipment—for instance, a control name or a specific "suite" number with the order. Use your imagination to create a personal code for all inbound packages.

Encourage close friends and family members to send you packages only after advising you by telephone or mail that the item will be sent. One useful technique is to assign specific friends and associates a different code identifier in the address you give them, and always verify this code when the package arrives. If there is any question, always call and verify that the package was sent.

For letters and general correspondence, code identifiers can be used just as easily. Somewhere on the envelope a specific code should be used to verify the validity of the sender. One useful technique is to advise friends and family members to include a specific code in the return address on all correspondence. A simple and deceptive measure is to add a preestablished four-digit number to the end of the sender's ZIP Code, or a specific suite or apartment number to the return address.

For a high-threat situation, it is sometimes useful, as well as very "friendly," to include a self-addressed stamped envelope to certain family members and friends for use when writing back. Always leave the return address space blank so the sender can write in his or her own hand the return address and code identifier. This secure approach to correspondence is also somewhat conducive to getting certain friends or associates to respond to your letters a bit faster, since the return envelope is in front of them and ready to go.

Keep records of shipping labels and stationery used by regular correspondents so that you can

instantly recognize them. Keep all records of expected shipments as well as direct access to your correspondence and shipments secure from surveillance and tampering.

Discard anything suspicious at the post office. If you do in fact suspect that a specific package may contain an IED, quietly ask to speak with the postal inspector, and advise him privately of your suspicions. If you do end up with a suspicious letter or package in your home or office, there are some important things you should and should not do.

First, you should not handle it too much or attempt to probe or otherwise physically inspect it. Package bombs, by their very nature, are somewhat resistant to rough handling, since the killer must consider the amount of abuse and environmental exposure the package will have to go through in order to make it to your mailbox. But you should still be careful.

Another very common and increasingly deadly mistake is the belief that a package or letter bomb somehow can be neutralized by immersion in water or other liquid. Many movies and television programs perpetuate this foolish technique.

The overwhelming majority of package and letter bombs is designed to explode upon opening. This is generally accomplished through the use of a mechanical, electrical, or chemical release mechanism. It may be a pressure-release or spring-loaded switching, system or a friction-related ignition configuration. Regardless of the nature of the device, if it is immersed in water, the cardboard or paper wrapping will get soggy and its strength will degrade rapidly. The pressure release or other ignition sequence will then occur and detonate the charge.

No bucket or other container typically available in a home can safely hold enough water to protect the area from the effects of the blast. In fact, in some instances the container may actually shatter, causing a large number of secondary fragments to burst outward from the device.[8]

Containment of the letter or package can be accomplished by placing it outdoors, away from people or vehicles, in an area where EOD (explosive ordnance disposal) personnel can safely examine it. If the device came in the mail, there is little risk in moving it a few hundred feet to a safe area.

If the package is personally delivered to your doorstep or office, you are advised not to touch it or go near it. One useful, but perhaps cruel, approach to addressing the delivery of an unsolicited package is to ask the person delivering it to open it himself from a safe distance. When operating overseas, all personnel should be advised to request the bearer of any unsolicited package to open it himself, outside the office or residence. This practice has resulted in individuals immediately fleeing with the suspicious package.

This approach may, of course, kill an innocent delivery person or, at the very least, cause legitimate package deliveries to be slowed down to a degree. Thus, it is seldom a realistic solution. It is more practical to have one person designated as the company's receiver of all package shipments. This person will come to recognize the various delivery drivers by name, and a new or suspicious driver bringing an unexpected package can be "handled" differently without interrupting the normal flow of packages into the business.

If your business has security personnel on staff,

they can be most helpful in establishing access-control procedures. One very useful approach is to have several well-posted signs indicating that all deliveries are to be made at a specific entrance to the building. This area should be somewhat isolated from most building occupants and designed to minimize damage from a blast. This can be accomplished without causing undue stress or anxiety to the person receiving and logging packages if it is done discreetly and is focused on his protection as well as that of the delivery driver.

Security personnel should never be asked to inspect or open a suspicious package. Most security personnel are not trained or equipped for this task, although experience indicates that many will courageously attempt to inspect or open a suspicious item in order to protect the person making the request. This situation should be considered during the planning stage and eliminated from becoming a likely possibility.

The only realistic containment procedure for a suspicious delivered package is the use of a bomb blanket. These ballistic coverings, often made of Kevlar, are the *only* things that should be placed on top of a suspicious package. Never surround the package with anything in hopes of containing the blast. You will only make its inspection more difficult for EOD personnel, and you may inadvertently use a containment device that will result in more shrapnel.

Your shipping and receiving area should have a bomb blanket and adequate fire-control equipment. A preestablished, written procedure for handling suspicious packages should be posted and read by all personnel in receiving. A contact person should be

specified in case a suspicious package is encountered. Again, as with a bomb threat, the person detecting a suspicious package should not discuss the discovery or the procedures with anyone.

Restricting access to your mail and packages from interception or surveillance, and establishing procedures to handle inbound letters and packages are vital elements to addressing the threat of a mail IED. (Obviously, you should control your outgoing mail with the same attention to security.) Common sense and careful planning can reduce the threat significantly.

Suspicious Package Warning Indicators

NOTE: RECENT BOMB ATTACKS USING LETTERS AND/OR PACKAGES DISPLAYED NO IDENTIFIABLE CHARACTERISTICS OR "TYPICAL" APPEARANCE. THERE ARE, HOWEVER, SOME DANGEROUS WARNING INDICATORS TO BE AWARE OF WHEN HANDLING ANY UNSOLICITED CORRESPONDENCE.

Letters

1. Letter is thick and stiff, and may be labeled to indicate that it contains photographs or the like, and to not bend it. This is an almost universal characteristic of most letter bomb IEDs. The stiff "feel" to the letter is designed to conceal the bomb's density or to prevent handling of its pressure-release device.

2. Letter has a "mushy" feel to it. This may be a liquid-cell battery used for detonation circuitry, or it may result from a sealed plastic charge designed to defeat "sniffer" detection systems. Plastic or sheet-type explosives have a density and feel of paraffin.

3. Envelope is oily or discolored. Plastic explosive tends to break down to its oil base when exposed to rough handling in various temperature extremes.

4. Letter has uneven texture, including bumps, wire, or unusual shapes.

5. Letter is packaged as though there is another envelope inside the actual mailing envelope. This is a very dangerous design configuration.

6. Letter is addressed by hand to a specific person. May have the words "confidential" or "personal" on the envelope. Beware of excessive postage on this type of letter. It is unknown why these types of letter bombs have many more postage stamps than would normally be required.[9]

7. Letter is mailed from another country or a distant state and, again, is addressed specifically to the target.

8. Letter is overweight. It feels heavier than it looks in terms of size and density.

9. Letter is "springy" and forms back to its original state when mild pressure is placed on the outside of the envelope and then released. Standard pressure-release devices will often have this characteristic.

10. Letter is over or undersized. It seems to be very thick for the size of the envelope.

11. Anything out of the ordinary about an unsolicited letter—an unusual odor or a strange "feel"—should be cause for concern.

Packages

1. Package is wrapped in a way that it cannot be opened for cursory inspection by the shipper. It is

frequently wrapped in brown paper with heavy tape or, more commonly, string or heavy twine.

2. Package feels imbalanced when held in the hands. One side is heavier or lighter than the other.

3. No movement or sound inside package when it is shaken lightly. Unlike typical merchandise or gifts from friends, a package IED must not be able to shift or move around in transit, so the contents are carefully secured inside.

4. Package can only be opened one way. For example, the wrapping terminates at one point (frequently on the bottom), the cardboard box has its bottom taped heavily so it must be opened from the top, and so on.

5. Package is heavy and seems dense in size and weight.

6. Package is meticulously wrapped and labeled. Every detail seems "too neat" or overdone in attention to detail.

7. Package was shipped from outside the country or from another state, and excess postage stamps were placed on the wrapper.

8. Package label is handwritten in large block letters, including the word "Personal" or some other message to discourage the package from being opened by anyone other than the addressee.

9. Anything unusual about the package should immediately arouse suspicion—a foul odor or any type of oily leak, a typewritten label from an old-style typewriter, excessive wrapping or tape, and so on.

Overview

The above checklist is based on post-blast evidence from letter and package bomb incidents. It is not intended to describe any specific type of

dangerous unsolicited package as much as it is meant to serve as a warning that a package or letter may seem "strange" in a manner that provokes only curiosity rather than suspicion. In fact, post-blast interviews with survivors of these types of attacks indicate that the victim thought the package or letter was "curious" but not at all suspicious.

It is very human to enjoy receiving packages and letters in the mail, particularly those that appear to have some type of emotional or intrinsic value. But you must be very careful when handling any unsolicited letter or package, and be alert to any type of labeling designed to mislead or provoke interest.

Letter bombs kill through concussion or massive burning, although many terrorist groups (and even certain intelligence agencies that meet the enemy on their own terms) tend to place just enough explosive charge to intentionally maim the victim. Package bombs generally kill through the heavy blast and fragmentation effect of the IED pressure vessel (such as a pipe bomb), as well as through the use of shrapnel, such as nails or tacks.

The majority of these devices explode upon opening. This requires some sort of pressure release or sensory circuitry. With post-blast evidence, the most pronounced and obvious component in a letter bomb is this release mechanism or circuitry. The most obvious component in a package IED is generally the charge housing and shrapnel.

If there is ever any doubt, don't attempt to open the package or letter. It is better to safely dispose of it rather than attempt to satisfy your curiosity.

AREA BOMB PLACEMENT PROTECTION

If you are difficult to surveil and your vehicle and mail seem to be unlikely media in which to employ an IED, then the placement element has only one choice left. He knows where you live and where you work or conduct business. Unless you hide in an underground, concrete-reinforced bunker, you can still be a target for an area-emplaced bomb.

No matter when you leave home or work, and no matter where you go, it is likely that you will eventually return to a few specific areas almost every day. Once the diligent surveillant recognizes this as being the only predictable aspect of your behavior, he will attempt to arrange an ambush between you and an IED at one of these normal destinations.

Access control is important in protecting a specific area from an IED placement. In a business or location that has a steady flow of customers or pedestrians, access control must be employed with a means of hardening all threat areas that, by nature, are difficult to secure from random, unsupervised access.

The first step is to perform an area assessment. It is important to understand the motivations behind an IED placement mission, as well as the technical requirements for most such operations:

1. The placement element must be assured in advance that the area will be accessible without challenge or suspicion.
2. The IED must be concealed in a wrapping or location where it will not be detected prior to detonation.
3. The placement is intended to kill specific

targets or cause structural damage from the blast or post-blast fire.

4. The IED must generally be command or time-sequence detonated. It is frequently armed prior to emplacement.
5. The individual assigned the task of placement may or may not be aware of what he or she is carrying to the target area. The use of unwitting agents is becoming more common, but regardless of his or her knowledge, the conduct of the individual assigned the task must appear "sterile" to security personnel in the area.

With knowledge of the above five points, consider the vulnerable areas of your home or business and privately plan a mock "bomb placement mission" on your property.

Start with those areas where you have no means of controlling access—specifically, outside your building and the surrounding grounds. Most area bombs are placed outside the target building close to the most sensitive structural area, such as a window or door. The device may be placed in a trash container or pushed into a mail slot, for instance. It may be packaged in a manner that causes a curious interest, such as a labeled box.

One recent technique used a newspaper rolled up to conceal a pipe bomb, which detonated when picked up by the target, who had been observed doing this as part of his morning routine. Another booby-trap device was placed in the trash can of a victim who was known to personally take his cans to the street for morning pickup.

The important thing to do is to secure the area. Have the grounds free of clutter or debris. Keep lawns and flower gardens neatly clipped and hedges

trimmed, and clear fences or other obstructions that could be used by a burglar or attacker to provide cover for himself or an IED. Consider having a large dog capable of living outdoors most of the time. Invest in good outdoor lighting, as it is an excellent deterrent to any sort of crime.

Do not have a "doggy door" contraption that is accessible from the outside. Fill and block any mail or delivery slots. As an alternative to power-hungry lights, consider infrared security lighting that "locks on" the ambient temperature of a large mass, but that also has a means of audibly alerting you to the fact that the lights went on. An RF pager device connected to this setup may be useful as well, which could both alert you to an intruder and prematurely set off a blasting cap in an IED.

Keep all containers such as trash cans, flower pots, and lawn displays away from the house and inaccessible to anyone but members of the household. Advise all delivery personnel that nothing is ever to be left on your doorstep if you are not home. Do not accept morning paper delivery or any other type of delivery service where the pickup or drop-off is done without your knowledge or participation.

Your area security should be focused on physical barriers and perimeter sensory devices designed to detect activity or intrusion. A small but loud dog is probably much better than a sophisticated security system that is likely to be too complicated or unreliable to be effective.

Perform a "walk through" around your residence or business and your risks will become obvious. Be particularly aware of parking areas where an unauthorized vehicle can be left near your building. Install signs or barriers to prevent such activities.

Any vehicle not belonging near your business or residence should be towed by the police after being reported as abandoned.

One useful and highly educational "field trip" to consider is a visit to your local shopping mall or large airport. Architectural designs of modern public-access areas are clearly becoming more focused on security threats from IED placement. Notice that public areas have signs posted indicating regulations and prohibited activities. Note that the furniture in all rest areas in malls and airports may be comfortable, but, more importantly, it can't be pushed or have something concealed in it. Notice the trash receptacles are large, stout designs that don't hold a lot of trash. Small flower gardens and atriums are neatly spaced and have the plants pushed back from the edges.

The point is that anything left unattended in these areas is obvious, and thus is "corrected" immediately. From a piece of litter to an abandoned bag, everything is closely observed and quickly "cleared" by security or maintenance. The most useful strategy appears to be neatness and an orderly design layout. This allows immediate observation of anything out of the ordinary.

You can apply these same techniques in your business. Plan a security assessment of your public rest rooms. For paper debris, use a small, see-through trash can such as a clear plastic or wire-mesh type. Secure the back of the toilet or place a physical barrier under the lid. Make sure towel dispensers and service closets are locked and secure. Again, focus on cleanliness. Designate one employee to regularly inspect the rest room for cleanliness and remove all debris.

Just as a clean vehicle is difficult to tamper with without leaving evidence behind, a clean and orderly area is an excellent deterrent to an IED placement. Whether you are securing a parking lot, rest room, garage, or warehouse, there should be a well-established order about everything. Anything out of place should be immediately obvious to the occupant. A bomber who recognizes a diligent focus on maintenance and cleanliness will have trouble planning a placement mission.

If you are not intimately familiar with your building, then enlist the maintenance or service personnel to show you around. Carefully study your area from a bomber's perspective. Ducts and ventilation grills should be secured. No area should allow quick concealment of a small package. Posted signs on doors such as "Employees Only" and "Private" also promote an image of awareness.

As should be obvious by now, access control means denial to and physical security of all areas. An efficient area assessment considers the most likely target, either human or structural, and then eliminates the placement opportunities. If you have read this book completely and carefully, you should have adopted some of the mind-set that goes into a bombing mission. Use this knowledge to deny both access and opportunity.

Conducting a Bomb Search

When a bomb threat has been received, many agencies have preestablished procedures for a thorough search of the premises. In fact, unless a clear and present danger of an imminent detonation has been communicated, then the search is typically conducted prior to making the decision to evacuate.

You may wish to consider this approach as well. The guidelines in this section are intended to assist you in developing a search plan.

There is one very major decision you must make prior to executing a search for a suspected device. The question in your mind ought to be, "What am I going to do if I actually find a bomb?" The reality is that in many modern IED threat scenarios, the actual target is the person who is tasked with "attacking" the IED to render it safe. If someone communicates a bomb threat and gives an exact description and location of the IED, he simply may want to protect human lives, or he may wish to get someone close to the device for a command detonation. Sensory circuitry that is simple to design and install on an IED can detect sound, motion, or body heat. The bomber may wish to ensure casualties by placing a sophisticated booby-trap device designed to detonate only when humans are within the lethal blast zone.

The bomber may also have planted more than one IED on the premises. Once the search team has located the bomb and the EOD operators have neutralized the threat, other devices may be in place to explode in the area.

The point is simply that unless you are highly skilled, unable to get assistance, or unable to evacuate the area, you probably have no business attempting to search for an IED. In fact, many actual cases brutally demonstrate the reality of bomb placements designed to detonate at a specific time or when visually discovered.

After explaining all of the potential risks, why have a section on bomb searches at all? Because the time to perform a detailed bomb search is right

now—*before a bomb is emplaced.* Carefully explore your home and work environment, looking for areas where it would be easy for someone to conceal a device about the size of a pack of cigarettes without being observed, challenged, or detected. Make note of all of these "hides" and methodically eliminate access to them. Address denial of obvious opportunity as well. You can creatively deny the placement of a device by carefully considering where *you* know for a fact one could be easily concealed in your environment.

It may get somewhat overwhelming once you realize the potential danger areas around you. Simply prioritize each threat area and address them to the best of your ability.

If you have a close friend, trusted employee, or family member, a serious game of "hide and seek" can be played with a small package. This has been determined to be an excellent means of target hardening to a very high degree. The imaginative study of an area and careful concealment of a device requires a form of preattack surveillance that is not likely to be afforded to any opponent on the scale it will be to you.

Once it becomes difficult to find places to stash a small package, it will be because you have installed detection devices and physical barriers where needed and conducted a careful cleanup of your environment that effectively and efficiently denies access and opportunity.

Most importantly, a bomb search as a training tool is like kata in martial arts or weekend visits to the range in combat handgunning. It makes you aware of the threat while actually practicing the skills necessary to address and neutralize it prior to

the encounter.

Make careful notations and sketches of your property, and develop a documented procedure for a thorough search. This has been found to be highly useful for the EOD search element should a threat ever arise and a thorough search need to be conducted. Remember, no one knows the building better than the regular occupants. If a search team has access to detailed notes and blueprints or schematics of the premises, as well as advice from a maintenance supervisor on the building's structural details, the entire operation is faster and much safer for everyone concerned.

CONCLUSION

The threat of an IED placement can be effectively addressed with the procedures and strategies outlined in this book. The operational characteristics of a bombing scenario were carefully considered in formulating the countermeasures described herein.

As a student of such behavior, I believe that it is unlikely that the IED threat is going to abate any time soon. Some of the procedures outlined in this book are considered objectionable by many colleagues because they focus on capturing or killing the bomber while, at the same time, protecting the principal or property.

Unfortunately, the tragic reality is that we are forced to learn about IED threat management "one blast at a time." Since access to the four thousand chemical compounds that can react explosively with one another cannot be controlled effectively, and since the behavior or intention of a bomber cannot be predicted, it comes down to each individual taking steps to not only discourage such behavior through

threat management, but also to continuously capture or intentionally kill those who try.

The only "good" explosion is when the only victim is the individual or group attempting to construct, transport, or emplace an IED against his fellow man. The bomb has become a media-sensationalized, politically "acceptable" form of expression. The use of countermeasures that "help" the terrorist or criminal die for his cause is a tragic reality of addressing the threat effectively. Despite objections from some of my colleagues, it seems to be the general consensus that this deadly approach is at least "fair" and fundamentally correct.

The author would be very interested in hearing from readers who have an opinion, criticism, or contribution to make regarding this text. Forward your comments to Paladin Press in care of the author. Any creative, optionally confidential contribution that you would care to make will be carefully considered and credited in future projects.

Finally, should you find that the use of this text or your own devious imagination is at all instrumental in identifying and/or capturing an individual who likes to play around with IEDs at the expense of his fellow man, do the rest of us a favor and ensure that this person is incapable of continuing such conduct ever again.

ENDNOTES

1. 1988 FBI Uniform Crime Statistics. This figure does not include acts of terrorism against U.S. citizens overseas. The statistic is an analysis of weapons used in homicide cases throughout the United States.

2. Bomb data statistics indicate that the likely victims in many IED situations are young males between 15 and 25 who attempt to construct homemade bombs using household chemicals or reloading powder. Many have a rudimentary knowledge of chemistry and, as a result, combine one or more chemicals that react violently. Also, many homemade booby-traps tend to injure, permanently maim, or kill the person constructing or transporting the device. Attempts by teenagers to use outdated underground bomb-making books, some that contain misprints or other erroneous information, also cause injury and death each year.

3. It is a felony to illegally record a telephone conversation without the consent of both parties. It

will make no difference if the individual placing the call has threatened you. Do not employ line voice recording if you are likely to be caught doing so. However, though the use of the recording as evidence is unlikely, its intelligence value is quite high.

4. In the United States and Europe, when power is removed from any natural gas appliance, the gas regulator will automatically shut down the flow of gas. However, this must be verified with the building maintenance or serviceman for the specific systems in your structure. Note also that the main circuit breaker is generally the ideal shutoff point for these devices.

5. Experience has shown that an individual who communicates a legitimate bomb threat is doing so only to save human lives and/or to claim responsibility for the attack in advance. In Great Britain, for instance, the Irish Republican Army (IRA) has made arrangements with the military and law-enforcement agencies to provide a code word in communicated bomb threats that indicates that the threat is real and legitimately from the IRA. It is important to stress to all personnel likely to process the threat to sound compassionate and concerned with saving lives. This is very helpful in dealing with legitimate threats.

6. A fake video camera is simple to detect. Yet these popular devices are seen in high-risk locations, presumably for their deterrent value. Real video cameras emit an oscillation that can be heard in the speaker of a small AM radio or Walkman. Simply holding an AM radio close to a fake camera will

clearly demonstrate the deception. Thus, fake cameras are basically worthless and perhaps even legally negligent to employ. (Terrorist training camps in Libya have made this simple detection technique part of their training doctrine since at least 1983.)

7. Cordless telephone monitoring is extremely easy to accomplish using off-the-shelf hardware. The Electronics Communications Privacy Act (ECPA) does not protect these conversations from interception and recording. In a February 1990 Supreme Court ruling, it was established that the user of a cordless telephone does not have "a reasonable expectation of privacy" when talking on such devices. Law-enforcement agencies and private investigators exploit this technical loophole to conduct creative wiretaps on targeted individuals.

Cellular phone conversations are perhaps slightly more secure, but these too can be intercepted using off-the-shelf hardware. The cellular phone industry has perpetuated the image of a car phone as being secure, difficult to intercept, and legally protected. This is simply not true. It is speculated that certain law-enforcement agencies and private operatives encourage the false sense of security provided by cellular phone use.

8. The now well-established trick of viewing the contents of an envelope by spraying the outside with Freon may have limited use in noninvasive postal intercept, but this technique should *never* be used to view the inside of an envelope suspected of containing a mail bomb. The Freon causes the envelope to be temporarily transparent, allowing an individual to view its contents. However, it also

adversely affects the tensile strength of the envelope, which may cause a pressure-release device to pierce the wet paper and detonate the charge. Also, the pressurized can of Freon in your hand will become a secondary explosive container. This technique is perhaps best relegated to amateur undercover investigations and spy novels.

9. It is a typical operational technique to mail a letter bomb by placing it into a mailbox without being observed and as anonymously as possible. This precludes taking the letter to the post office. It had been thought that the excess stamps were simply "insurance" for the sender, who perhaps, not knowing the exact weight or postage required for the letter, simply placed extra stamps on the envelope to ensure its arrival.

More recent psychiatric studies and intensive forensic analysis of individuals who have been convicted of sending mail bombs tends to disqualify this theory. Most convicted bombers took great pride in the detail of their surveillance and the design and packaging of their devices. They frequently were meticulous personalities who often knew the exact weight and required postage for the letter or package they sent. One individual went so far as to choose a specific type of stamp for his package, which he selected based on the known interests of the target.

Yet none of the individuals interviewed could provide a reasonable answer as to why they placed excess postage on their bomb packages. It is notable that while many letter bombs seem to have this characteristic, it is not a universal or even typical pattern in many recent attacks.